Leni freire Joaquim Varela

Forense Computacional em servidor IIS 5.0

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

3.1.12

Leni Freire Joaquim Varela

Forense Computacional em servidor IIS 5.0

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

3.1.12

Leni Freire Joaquim Varela, autor da monografia intitulada Forense Computacional em servidor IIS 5.0:, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia aos 30 de Setembro de 2010
Leni Freire Joaquim Varela

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Engenharia de Sistemas e Informática.

Lista de Acrónimos

DoS – Daniel of Services (Negação de Serviços).

DDoS – Distributed Denial of Services (Negação de Serviço Distribuido).

IDS - Sistema de Detecção de Intrusão.

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança.

IIS - Internet Information Services.

NCSA - National Center for Supercomputing applications.

IIS - Internet Information server.

W3C - World Wide Web Consortium.

UTC - Universal Coordinated Time (Tempo Coordenado Universal).

ASP - Active Server Pages (Páginas de Servidor Ativas).

Sumário

Nas últimas décadas a utilização de computadores tornou-se parte integrante da vida das pessoas, permitindo o aparecimento de vários tipos de crimes electrónicos. Neste contexto, é importante que as organizações se preparem para investigar casos que envolvem a informática e adoptem procedimentos válidos e confiáveis que permitem recuperar os dados dos computadores envolvidos em actividades ilícitas. A Forense Computacional, são técnicas que permitem-nos recolher, identificar, analisar e apresentar evidências de crimes digitais.

Pretende-se com este trabalho, apresentar as principais técnicas de Forense Computacional em servidor IIS 5.0 da Microsoft.

Palavras-chave: segurança, Forense computacional, evidências, Servidor IIS.

Agradecimentos

A Deus que esteve sempre comigo durante esta empreitada.

A minha mãe pela confiança, amor e carinho transmitidos a mim durante toda a minha vida.

Ao meu orientador Isaías Barreto Rosa pela oportunidade, atenção e aprendizado.

Em especial aminha esposa Samirapelo amor, companhia, amizade, incentivo, discussões enriquecedoras e sobretudo por ter me apoiado muito tanto no mundo virtual com no mundo real.

E a todos que contribuíram para a minha formação, especialmente a minha filha Alysa e aos meus familiares.

Conteúdo

Tabelas

Figuras

CAPÍTULO 1: INTRODUÇÃO

1 Contextualização

O presente trabalho, intitulado "**Forense Computacional em Servidor IIS 5.0**" propicia o estudo de um conjunto de técnicas que possibilitam a investigação de crimes praticados nos mesmos.

Com o desenvolvimento das tecnologias de informação e do acesso cada vez maior da população às suas facilidades e serviços, alguns aspectos na vida sofreram profundas transformações, tais como a difusão de dados, as transacções comerciais e bancárias, a segurança de dados cadastrais, entre outras.

Por consequente, os prejuízos causados à sociedade e empresas são enormes, havendo a necessidade de combater essa nova modalidade criminosa.

Nesta óptica, surge a necessidade do uso de técnicas de Forense Computacional que nos permite conduzir uma investigação estruturada com uma metodologia que possa determinar o que acorreu, como ocorreu e quem foi o responsável.

2 Objectivo

Este trabalho tem por objectivo apresentar um Estudo da Forense Computacional em Servidor IIS 5.0.

Os objectivos específicos são:

- Descrição detalhada sobre onde, como e o que procurar em um servidor web sistema comprometido;
- Instalação, configuração e disponibilização de um servidor web para eventuais ataques;
- Recolha, análise e apresentação de evidências;
- Apresentação de ferramentas de investigação de crimes digitais;
- Enquadramento legal das evidências

3 Motivações

- Porque os servidores webs são as principais vitimas de ataques realizados por meios da internet;
- E por ser a Forense Computacionaluma ciência que permite estudar e obter provas de crimes digitais.

4 Estrutura do trabalho

O trabalho está dividido em 5 Capítulos:

No capítulo 2, **Segurança Computacional**, serão apresentados alguns aspectos fundamentais de segurança como as ameaças, vulnerabilidades e as formas de ataques aos sistemas informáticos. Também serão apresentados alguns aspectos legais.

No capítulo 3, tema principal deste trabalho **"Forense Computacional em Servidor IIS 5.0"**, serão apresentados um conjunto de técnicas forense utilizadas durante uma investigação após intrusão. Também será explicado detalhadamente toda a parte teórica sobre o funcionamento de servidor web, desde arquitectura, instalação, configuração, segurança, arquivos de log e a auditoria no IIS. Este capítulo servirá de base para desenvolvimento do estudo de caso.

No capítulo 4, **Estudo de caso**, será apresentado um estudo de caso prático, dividido em duas partes: uma em que será montada um servidor web (correndo o serviço IIS 5.0) e disponibilizado na internet para ataque; e a parte de investigação forense no servidor comprometido.

No capítulo 5, **Conclusão**, procura-se de uma forma bem resumida, mostrar a importância da forense computacional no tratamento dos incidentes de segurança e uma análiseda lei no domínio dos crimes informática em Cabo Verde.

Na **Recomendações**, será feito algumas recomendações no domínio da segurança, dos espetos legais e sobre as boas práticas de investigação forense.

CAPÍTULO 2: SEGURANÇA COMPUTACIONAL

O presente capitulo aborda a relação entre a evolução da tecnologia no mundo e consequentemente o surgimento de novas formas de crimes realizados por meios de computador. Ainda abordaalguns aspectos relacionados com segurança da informação, ataques e vulnerabilidades de sistemas e a necessidade de novas leis. Esses itens são a motivação principal para o surgimento da forense computacional, o temo deste trabalho.

1 Contextualização

À medida que a tecnologia progride, novas vulnerabilidades vão surgindo. Por isso, torna-se necessário ter conhecimento geral destas vulnerabilidades ou pontos fracos de forma a se prevenir melhor das ameaças e assim reduzir os impactos que possam causar.

Neste contexto, é necessário a utilização de um conjunto de mecanismo de segurança que permite a sua protecção contra os potenciais agressores.

1.1 Protecção da informação

A informação tornou-se uma necessidade crescente para qualquer sector da actividade humana. Também, por assumir, hoje em dia, uma importância crescente e fundamental sobretudo a nível da empresa, é necessário estabelecer politicas de segurança como forma de garantir a sua protecção contra a sua utilização mal intencionada ou agressores.

Segundo Bueno (2007), a protecção da informação é o objectivo principal das áreas relacionadas à segurança da informação. Para o mesmo autor, proteger dados computacionais significa assegurá-los de destruição e comprometimento.

Para proteger tal conteúdo, é usado vários mecanismos de segurança, como a autenticação, confidencialidade, integridade, controlo de acesso, entre outros. Uma outra forma de proteger a informação é aplicar a manutenção da segurança, pois, esta impede a informação de ser perdida.

2 A evolução da criminalidade e evoluçãotecnológica

A evolução da tecnologia e sua popularização, tem sido, de uma forma geral, a uma velocidade muito maior que a legislação preventiva, situação esta que causa grande preocupação. Com isso quer-se dizer que a sua evolução está proporcionando uma dimensão da criminalidade, pois a criminalidade tecnológica aumenta em proporção da tecnologia.

Como podemos observar, a tecnologia dos computadores está envolvida em um número crescente de actividades ilícitas comoa invasão de sistemas, os delitos e fraudes informáticos, a disseminação da pornografia infantil e entre outros.

O caso do Brasil

Brasil, é um exemplo de País considerado como a referência mundial em crimes cometidos via internet. As estatísticas revelam que o Brasil é o país com o maior número de hackers especialista no mundo.

Segundo dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), a evolução dos crimes virtuais causados por ataques

(invasões, scan, fraude, ataques a servidores web e Denial of Service) aumentaram progressivamente de 3107 no ano 1999 para 358343 no ano 2009 e, com uma diminuição brusca para 61147 no ano 2010 como mostra a figura a seguir:

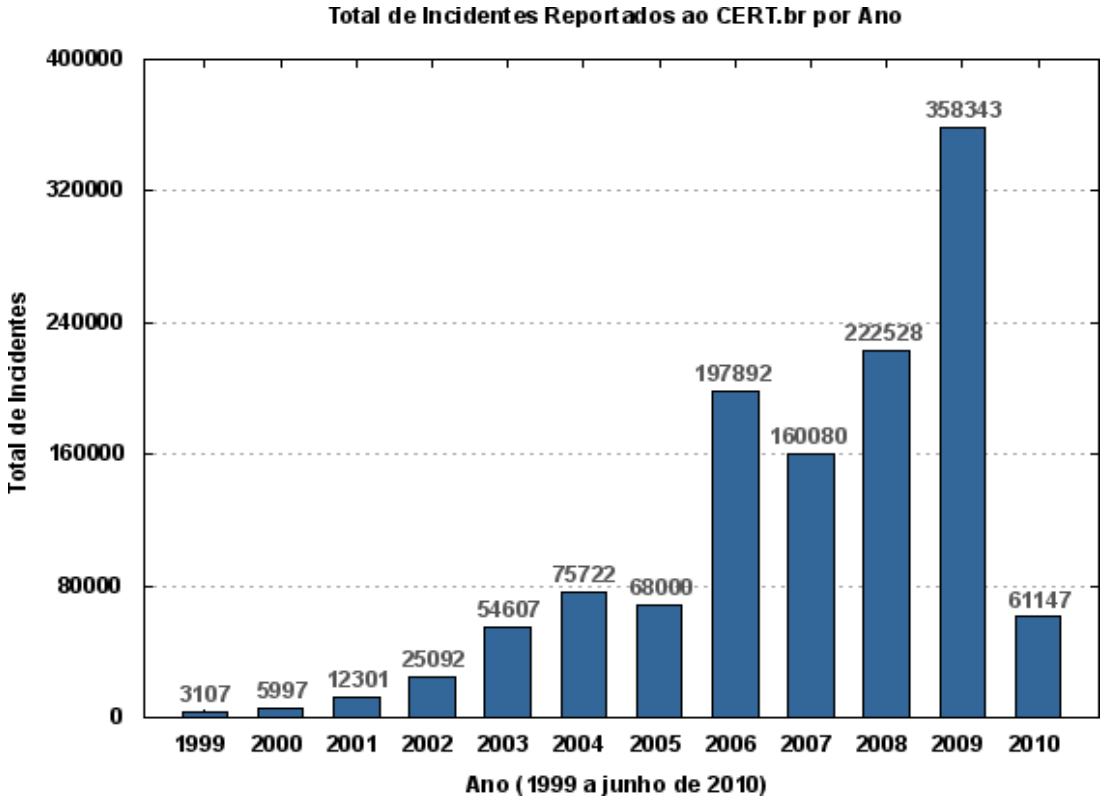

Figura 1 - Evolução dos Incidentes de segurança – Brasil

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Disponível em: http://www.cert.br/stats/incidentes/

Como podemos verificar, no ano 1999 houve um número total de 3107 incidentes, e segundo a CERT.br, dos 3107 incidentes, 4 correspondem a fraudes, 21 correspondem ao DOS (Denial of Service), 128 corresponde a invasões, 183 corresponde ao aw (ataques a servidores web), 658 correspondem a af (Ataque ao usuário final), 845 correspondem a axfr (tentativa de obter/actualizar mapas de DNS) e 1268 correspondem a scan.

O ano 2009 foi o ano com maior número de incidentes até a presente data, pois atingiu um total de 358343 incidentes. As fraudes aumentaram para 250362, DOS para 896, invasões para 111, scan para 52114, web para 5592, worm para 45099 e 4169 correspondentes a outros tipos de ataques.

Já no ano 2010, tais incidentes tiveram uma diminuição brusca de 358343 em 2009 para 61147 em 2010, com um número total de worm correspondente a 4761, DOS a 5, invasão a 12, scan a 17023, web a 1881, fraude a 8060 e um valor total de 1080 correspondente a outros tipos de notificações de incidentes que não enquadram na categoria anteriores.

O caso dosE.U.A

De acordo com a pesquisa "2004 E-Crime Watch", conduzida pela revista CSO com o apoio do serviço secreto dos Estados Unidos e do CERT, em 2003, invasões, ataques, disseminação de vírus, spams entre outras actividades considerados crimes digital custaram às empresas Norte-Americana um valor total de 666 milhões de escudos US.

Um novo estudo realizado pela verizon com dados do Serviço Secreto dos EUA, o chamado "2010 Verizon Data Breach Investigations Reporter", oferece um quadro bastante amplo da natureza e das causa do cibercrimes em vários países do mundo. O estudo destaca a participação de funcionários das empresas, na chamada "engenharia social" e participação cada vez maior do crime organizado neste tipo de delito. Porém, em termos gerais, o número de crimes com dados electrónico caiu em 2009, em comparação com anos anteriores.(fonte: http://tecnovarejo.blogspot.com/2010/08/varejo-e-alvo-prioritario-de-crimes.html)

Segundo a mesma fonte, o Varejo está entre os três sectores mais afectados pelo furto e vazamento de dados sigilosos (informações privadas de consumidores, como documentos e números de cartões de crédito), representando 15% do total de crimes. O sector financeiro lidera com 33% dos casos, seguido pela área de hospitalidade e hotelaria com (23%). Ainda, a inclusão de dados do Serviço Secreto do governo americano, que investiga crimes financeiros, permitiu que o estudo incluísse e comparasse dados sobre crimes electrónico ocorridos nos últimos seis anos. O estudo inclui mais de 900 ocorrências, que causaram quase 1 milhão de dados sigilosos roubados.

Entre as principais conclusões do estudo estão:

- A grande maioria dos vazamentos de dados (69%), foi comandada por fontes externos, enquanto apenas 11% incluem a participação de parceiros comerciais;

- Quase metade dos crimes (49%) foram causados por agentes internos, um crescimento significativo que o estudo atribui à inclusão de dados do Serviço Secreto;

- 48% dos vazamentos foram atribuídos a utilizadores que abusaram do seu acesso privilegiado dos dados empresariais, com intenções criminosas. Quase 40% dos casos tiveram a participação dos hackers, enquanto 28% foram causados pela manipulação de contactos sociais e 14% resultou de ataques físicos a computadores de empresas;

- Assim como nos anos anteriores, quase todos os casos de 2009 indicam o furto através de servidores de aplicativos online, e 85% dos casos foram considerados de "baixa dificuldade" pela pesquisa;

- Um dado importante é que 79% das vítimas não adaptavam o padrão de encriptação PCI-PSS, considerado o mais importante para a protecção de dados privados.

E para finalizar, a queda do número total de casos em 2009 em comparação a 2008 é atribuída a uma série de factores, incluindo uma maior eficiência das políticas de segurança, tanto públicas como privadas. O estudo não detectou nenhuma correlação entre o tamanho de uma empresa e o seu risco de sofrer um ataque cibernético. Segundo os pesquisadores da Verizon, os criminosos geralmente escolhem seus alvos em função do possível valor do furto e do custo do delito, sem dar grande importância ao tamanho e localização da vítima.

3 Ataques e vulnerabilidades

Segundo (Bueno, 2007), organizações públicas e privadas são, constantemente, alvo de ataques de todo o tipo. Um levantamento realizado por (Icove et al, 1995) indica, segundo Bueno, que informalmente contabiliza-se que as perdas financeiras atingem a bilhões de dólares. Por outro lado, neste mesmo estudo, foi mostrado que esses ataques são praticados não apenas por pessoas de fora da organização, mas também pelos próprios funcionários da empresa, como mostra a figura abaixo. Muitas vezes os funcionários demitidos promovem ataques a sistemas como forma de vingança.

Também as vulnerabilidades de hardware e software podem incluir actos ilícitos como roubo e destruição de activos de rede e até mesmo softwares proprietários. Geralmente, esses crimes

não são enquadrados, juridicamente, em uma legislação especifica sobre crimes de computadores. Normalmente esses crimes são enquadrados na violação da integridade do património, pois o autor do crime não fez o uso direito da tecnologia de informação, nem da comunicação computacional para cometer o acto ilícito segundo (Da Silva Rodrigues & Caricatti, 2004) citado por (Bueno, 2007).

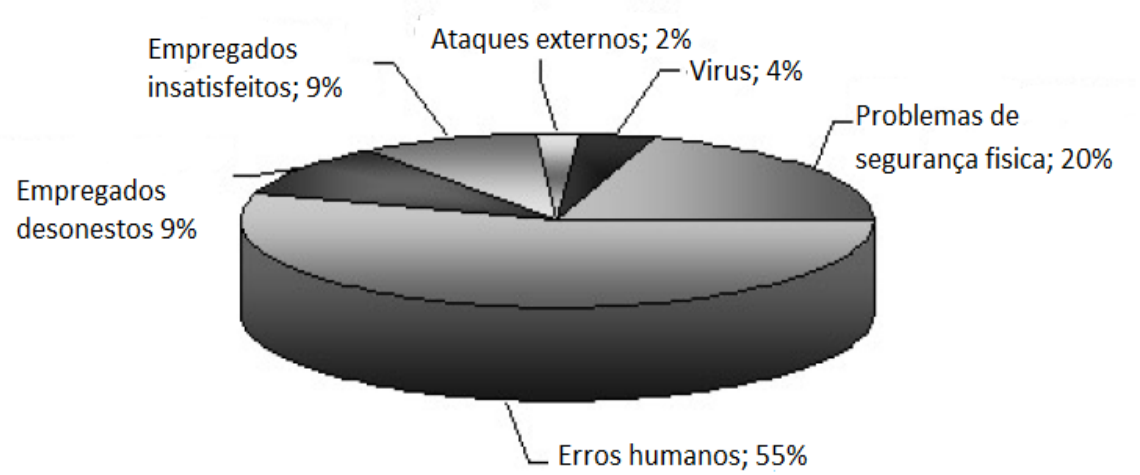

Figura 2 - Factores principapais de crimes e perdas
(adaptado por Icove et al, 2005)

3.1 Formas de ataques e invasões

Backdoors

Para (Lim-Apo, 2004), um backdoor é um mecanismo sorrateiramente introduzido nos sistemas de um computador para facilitar o acesso não autorizado a este sistema. Portanto, eles podem ser instalados para acessar vários recursos e são mais frequentemente instalados pelos atacantes que tenham comprometido um sistema para tornar mais fácil o seu retorno ao sistema, preferencialmente de forma menos visível.

Segundo o mesmo autor, alguns dos tipos mais comuns de backdoors tem propósito de disponibilizar serviços tais como: SSH, Rlogin, Telnet, FTP, Root prompt, Nasper, Gnutella.

Cavalos de tróia

Cavalo de Tróia, segundo (Lim-Apo, 2004) é um programa destrutivo que se apresenta aparentemente como uma aplicação benigna. Diferentemente dos vírus, este não se replica por se só, mas pode ser tão destrutivo quanto um vírus.

Ainda, segundo o mesmo autor, alguns cavalos de Tróia podem vir em forma de protecção de tela, por exemplo, um protector de tela que captura as teclas pressionadas em seu teclado (keylogger) ou que captura a área da tela de cada clique dado por seu mouse (mouselogger).

Criptanálise

O objectivo da criptanálise é, descobrir textos ocultados usando cifras ou descobrir segredos usados em sistemas de cifras para ocultar um ou mais textos. Pode ser usado para: (Zúquete, 2010).

- Obtenção do texto original relativo a um dado criptograma;
- Obtenção da chave de cifra (ou de uma outra equivalente) usada para produzir um ou mais criptograma;
- Obtenção do algoritmo de cifra (ou de um outro equivalente) usado para produzir um ou mais criptogramas.

Ainda, segundo o mesmo autor, as técnicas de criptanálise são inúmeras e seria fatisdioso enumerá-las todas. Importa, no entanto, referir as formas de ataques criptanalíticos mais significativas:

- ***Ataques usando apenas o criptograma (ciphertextt-only attackes):*** Nestes ataques procura-se descobrir um texto original ou uma cifra (algoritmo ou chave) que originaram um dado criptograma, partindo apenas do conhecimento deste último;
- ***Ataques com conhecimento do texto original (known-plaintext attacks):*** Neste ataque procura-se descobrir parte do texto original ou uma cifra (algoritmo ou chave) que originaram um dado criptograma, partindo do conhecimento deste último e de parcelas do texto original;
- ***Ataques com texto original escolhido (chosen-plaintext attacks):*** Nestes ataques procura-se descobrir uma cifra (algoritmo ou chave) usados num sistema criptográfico, introduzindo no mesmo texto escolhido, analisando o criptograma resultante;

- ***Ataques com texto original escolhido de forma adaptativa (adaptative chosen-plaintext attacks):*** Estes ataques sãouma variante dos que usam texto escolhido; a diferença está no facto de parte do texto introduzido ser escolhido em função dos criptogramas obtidos anteriormente;
- ***Ataques com criptogramas escolhidos (chosen-ciphertxt attacks):*** Estes ataques são uma variante dos que usam texto escolhido; adiferença está no facto de se introduzir criptogramas no sistema criptográfico e analisar o mesmo a partir dos textos originais produzidos (ou a partir das reacções causadas pela recepção desses textos originais);
- ***Ataques do aniversário (birthday attacks):*** Estes ataques são uma variante dos que usam pesquisa exaustiva. Têm este nome porque, segundo o paradoxo do aniversário, conseguem chegar a uma solução num número de tentativas inferior, próximo da raiz quadrada do que à partida seria expectável.

3.2 A necessidade de novas leis

A popularização do computador e da internet passou a ser vista por indivíduos mal intencionados como mais um meio de realizar crimes.

Normalmente, nos Países mais desenvolvidos onde existe uma legislação forte contra os crimes electrónicos, os criminosos da internet tendem a fugir, pois já sabem que num país onde existe uma legislação forte serão facilmente sancionados no caso de cometerem delitos. Portanto, esses criminosos ao fugirem tem tendência em refugiar-se para os países onde não existe uma legislação específica para esses crimes, ou se existe, então muito fraco.

Em Cabo Verde, ainda não existir uma legislação específica que trata de crimes desta natureza, o que pode constituir uma grande ameaça.

Uma das formas de prevenção contra esse tipo de situação é investindo na legislação. Com isso, está-se a querer dizer que se o país tiver uma legislação forte, os criminosos mantêm em distância e até mesmo os provedores, um dos principais causadores desses problemas passarão a se preocupar principalmente quando ficarem a saber de que podem ser chamados

em juízos ou notificados para prestarem informações sobre eventos ocorridos dentro de seus sistemas.

CAPÍTULO 3: FORENSE COMPUTACIONAL EM SERVIDOR IIS 5.0

1 Contextualização

1.1 Introdução à ciência forense

Ciência Forense, segundo Sêmola (2007) é uma área interdisciplinar que aplica um amplo espectro de ciências com o objectivo de dar suporte, respondendo perguntas às investigações relativas ao sistema legal, mais precisamente ligadas à justiça civil e criminal. Entre seus desafios está a identificação do crime, o rastreamento das etapas que o precederam, a localização e preservação de evidências e a geração de documento de suporte legal.

1.2 Forense Computacional

Segundo Lim-Apo (2004), "*O termo forense origina-se do meio policial, onde peritos investigadores procuram analisar de forma minuciosa tudo que encontram na cena do crime*…"

Dentro do contexto electrónico, a Forense, segundo (Menegotto, 2004) compreende a aquisição, preservação, identificação, extracção, restauração, análise e a documentação de evidências computacionais. Este processo permite o rastreamento, identificação e

comprovação da autoria de acções não autorizadas como violações de normas internas e até mesmo crimes electrónicos".

1.2.1 Forense na web

Histórico e cache

Ao contrário dos cookies, fornece pouca informação conclusiva, os ítens de histórico e cache possibilitam tirar conclusões sólidas a respeito da navegação na internet realizada na máquina investigada. Esses dois itens foram criados, como um meio de permitir a navegação e facilitar consultas a itensrecém-conquistados. Desta forma eles podem ser usados na forense para reconstruir a navegação de utilizadores. Portanto, o histórico de um navegador de internet regista a lista de URLs acessados recentemente pelos utilizadores do sistema. O cache diz respeito a acumulação de conteúdos acessados, como páginas e imagem, na máquina do cliente (Bueno, 2007).

Segundo (Bunting & Wei, 2006) citado por (Bueno, 2007), de forma geral, cada navegador adopta uma forma diferente para guardar os registos de histórico de um utilizador. Por exemplo, no Internet Explorer é definido um arquivo de índice denominado **index.dat**, um para cada dia de navegação.

No Mozilla Firefox é definido um único arquivo "history.dat", o qual armazena todas as entradas dohistórico. Particularmente, no Windows os arquivos de índice não registam apenas páginas e arquivos da Web associados via Internet Explorer; quaisquer arquivos abertos dentro da própria máquina serão registado no seu respectivo índice. Por exemplo, arquivos de texto, imagens, MP3, etc acessados no dia XX serão inseridos no index.dat desse dia, porém usando o termo inicial file:/// para indicar que é um arquivo local (Bueno, 2007).

Localização em disco

Segundo (Bueno, 2007), no Mozilla Firefox, o histórico é armazenado na pasta abaixo (pode sofrer alguma alteração de acordo com a versão do navegador usado):

X:\Documents and Settings\<usu_ario>\Dados de aplicativos

\Mozilla\Firefox\Profiles\<nome-aleat_orio>\history.dat

Diferentemente do Mozila, no internet explorer, a localização dos itens de histórico, cache e cookies encontra-se nas pastas de acorde com a tabela abaixo:

Item	Localização
Cache (Temporary Internet File)	X:\Documents and Settings\<usuário> \ Configurações locais\Temporary Internet Files \Content.IE5
Histórico (History)	X:\Documents and Settings\<usuário> \Configurações locais\Histórico \History.IE5
Cookies	X:\Documents and Settings\<usuário>\Cookies

Tabela 1: Localização de artefactos do Internet Explorer (Bueno, 2007).

Internet Explorer

No internet explorer (IE), de acordo com (Bueno, 2007), temos à disposição, sem fazer uso de nenhuma ferramenta, dois itens:

Histórico: Compreende diversos arquivos de índice. Cada arquivo de índice é guardado no seu respectivo diretório e nomeado de acordo com a data que representa, por exemplo MSHist122010032220070323. Este é um arquivo binário e proprietário da Microsoft, mas pode ser visualizado facilmente os seus registos, pois essa informação é guardada textualmente. Outras informações não textual que estão guardados são, por exemplo, uma tabela de hash para que o navegador seja capaz de montar e exibir o arquivo de índice.

Cache: Compreende um arquivo de índice e alguns directórios (geralmente 4) para guardar o conteúdo da cache. Este tem estrutura similar à do arquivo de índice do histórico, ou seja possui uma tabela de hash e os próprios registos de cada item de cache, estes últimos guardados em forma textual. Nos directórios do cache estão presentes os arquivos acessados

no IE, como páginas, figuras e folhas de estilo. Desta forma, é possível fazer uma averiguação do cache apenas verificando o conteúdo desses directórios não sendo necessário fazer uso do arquivo de índice.

Cookies

Segundo (Kurose and Ross, 2006) citado por (Bueno, 2007), cookies são mecanismos utilizados pelos navegadores de internet com a finalidade de manter sessões HTTP de utilizadores durante a conexão cliente-servidor.

O conteúdo de um cookie é o seu próprio cabeçalho que pode apresentar diversos campos como: (Jones, 2005) citado por (Bueno, 2007).

Set-Cookie: <NAME>=<CONTENT>; expires=<TIMESTAMP>; path=<PATH>; domain=<DOMAIN>

Um exemplo de cookie gerado pelo addthis é:

Browser: Internet Explorer

Site(s): adecn.com/

Name(s): AEID

Value(s):
YjBiOGJhMmQ2MGFhNGZjYzg5MjE0Nzg4M2RhYWMyNzY=|NqOKL/1VcWXKQ YVeiasWY5TqIMcgtHszf+nC8DdRsLg=

Expires on: 07-02-2011 10:32:48

Created on: 11-08-2010 10:32:13

Secure: no

Cookie file:

C:\Users\Leni\AppData\Roaming\Microsoft\Windows\Cookies\leni@adecn[1].txt

No cabeçalho acima, verifica-se que se trata de um cookie de nome “AEID”, cujo o conteúdo é:

YjBiOGJhMmQ2MGFhNGZjYzg5MjE0Nzg4M2RhYWMyNzY=|NqOKL/1VcWXKQYVeiasWY5TqIMcgtHszf+nC8DdRsLg=, criado em 11-08-2010 10:32:13, e será mantido pelo navegador até 07-02-2011 10:32:48. Na última linha é apresentado o localização do cookie no disco: :\Users\Leni\AppData\Roaming\Microsoft\Windows\Cookies\leni@adecn[1].txt.

Existem várias formas de visualizar o conteúdo de um cookie, como:

- Extensões do Mozilla Firefox;
- Cookie monster.

1.3 Evidência Digital

Segundo Marcelo & Paulo (2002), o termo evidência digital refere-se a toda e qualquer informação digital capaz de determinar que uma intrusão ocorreu ou que prove alguma ligação entre a intrusão e a vitimas ou entre a intrusão e o atacante.

Conforme os mesmos autores, a evidencia digital não deixa de ser um tipo de evidência física, embora seja menos tangível. Ela é composta de campos magnéticos e pulsos electrónicos que podem ser colectados através de técnicas e ferramentas apropriadas.

Nas palavras de (Chaves, 2004), "…" "*A maior dificuldade no combate às condutas no meio electrónico é quando estas são praticadas por grandes profissionais. Estes costumam não deixar vestígios, utilizando-se de artimanhas de enganar a policia e dificultar a actuação dos peritos na sua identificação*.[1]"

A evidência digital apresenta características próprias e complexas, exigindo conhecimento especializado na sua recolha e utilização.

Normalmente, uma das grandes preocupações para os especialistas em novas tecnologias é a identificação da autoria efectuadas no meio electrónico.

[1] Disponível em: http://ceae.geness.ufsc.br/index.php?option=com_docman&task=doc_details&gid=592. Consultado em 16/09/2006

1.3.1 O Professional

Os profissionais que actua na área de forense computacional são indivíduos geralmente chamados de perito por terem um grande nível de conhecimento nesta área e por investigarem os crimes de natureza tecnológicos.

Nesse contexto, Lim-Apo (2004) defende que esses profissionais devem reunir um conjunto de características:

- Conhecimento e entendimento profundo das características de funcionamento de sistemas de arquivos, programas de computador e padrões de comunicação em redes de computadores;
- Familiaridade com as ferramentas, técnicas, estratégias e metodologia de ataques conhecidos, inclusive as que não se tem registo de ter ocorrido, mas que já são vistas como uma exploração em potencial de uma determinada vulnerabilidade de um sistema;
- Faro investigativo para perceber rastros sutis de acções maliciosas - Esmero pela perfeição e detalhes. Sempre deve haver rastros, mesmo que muito sutis;
- Entendimento sobre o encadeamento de causas e consequências em tudo o que ocorre num sistema para construir a história lógica formada por acções maliciosas ou normais que já tenham ocorrido, que estejam em curso e que possam vir a acontecer;
- Conhecimento da legislação envolvida;
- Conhecimento das directivas internas das empresas e instituições envolvidas no processo investigativo, com especial atenção às limitações como directivas de privacidade, sigilo e escopo ou jurisdição de actuação;
- Cuidado com a manipulação e preservação de provas legais em potencial, inclusive com uma metodologia de cadeia de custódia. O que não é visto como prova hoje pode vir a ser uma prova e então é bom ter sido preservada o suficiente para ser aceita em um tribunal.

- Noções sobre a psicologia dos atacantes em potencial a respeito de perfis de comportamento e motivações.
- Experiência ao examinar os rastros em um incidente perceber o nível de sofisticação e conhecimento de um atacante, especialmente interessante se o atacante usa subterfúgios para parecer menos capaz, como deixar rastros óbvios e parecer um ataque simples para ocultar acções maliciosas muito mais perigosas e muito mais escondidas.

Ouarantiello (1997) num dos seus artigos relatado por Rodrigues & Caricatti (2004)[2], reforça ainda a ideia de que *"...o especialista deve conhecer o entendimento do judiciário, sobre questões tais como as condições em que é valido o exame pericial, falsa perícia e posição funcional do Perito no processo, entre outras que afectam, directamente, sua actuação, pois sem evidencias não há crime*".

1.3.2 Metodologia Forense para obtenção de evidências

De acordo com Adams (2000) apud Vargas (2007)[3], actualmente já existem padrões metodológicos bem definidos e desenvolvidas pelo SWGDE[4] que seguem um único princípio: o de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiabilidade e a precisão das evidências. Esse nível de qualidade pode ser atingido através da elaboração de SOPs (Standard Operating Procedures), que devem conter os procedimentos para todo tipo de análise conhecida e prever a utilização de técnicas aceitas na comunidade científica internacional.

Obtenção e Colecta de Dados

[2]Disponível em:http://www.linorg.cirp.usp.br/SSI/SSI2004/Artigos/Art010_ssi04.pdf. Acessado em 01/05/2010.

[3]http://imasters.uol.com.br/artigo/6225/forense/pericia_forense_computacional_e_metodologias_para_obtencao_de_evidenvias/

[4]Scientific Working Group on Digital Evidence (SWGDE) - representante norte-americano na International Organization on Computer Evidence (IOCE).

Os procedimentos adoptados na colecta de dados devem ser formais, seguindo toda uma metodologia e padrões de como se obter provas para apresentação judicial, como um checkList, de acordo com as normas internacionais de padronização, citadas acima (Vargas, 2007).

Ainda, segundo (Lim-Apo, 2004), mesmo que não haja a intenção de usar em um tribunal as provas obtidas, os procedimentos devem ser formais e seguindo uma metodologia como se as provas obtidas fossem para serem usadas em um tribunal. Durante o andamento do caso outros acontecimentos podem provocar a mudança na intenção e levar o caso a um tribunal.

Identificação

Durante a identificação das evidências, é necessário saber separar os factos dos factores, que possam vir a influenciar ou não um crime, para estabelecer uma correlação na qual se faz um levantamento das ligações relevantes como datas, nomes de pessoas, autarquias, etc, dentre as quais foi estabelecida a comunicação electrónica Vargas (2007).

Preservação

Um Perito Forense Computacional experiente, de acordo com Kerr (2001) apud Vargas (2007), terá de ter certeza de que uma evidência extraída deverá ser adequadamente manuseada e protegida para se assegurar de que nenhuma evidência seja danificada, destruída ou mesmo comprometida pelos maus procedimentos usados na investigação e que nenhum vírus ou código malicioso seja introduzido em um computador durante a análise forense.

Análise

Na concepção de Kerr (2001), a análise será a pesquisa propriamente dita, onde o investigador se detém especificamente nos elementos relevantes ao caso em questão, pois todos os filtros de camadas de informação anteriores já foram transpostos Vargas (2007).

Ainda, de acordo Kerr (2001) citado por (Vargas, 2007), deve-se sempre ser um profissional atento e cuidadoso em termos da obtenção da chamada "prova legítima", a qual consiste numa

demonstração inquestionável dos rastros e elementos da comunicação entre as partes envolvida.

Geralmente, para a análise das evidências é utilizado sistemas automatizados que pode gerar relatório detalhado, contendo a descrição das evidências encontradas, apresentação de eventos relacionados com intrusão e a determinação de outras características particulares do ataque, como por exemplo, a origem e alterações deixadas no sistema comprometido. Portanto, a automatização do processo de análise forense possui efeitos mais amplas, pois, à medida que a quantidade de informações armazenadas nos sistemas computacionais aumenta, essa automatização torna-se uma necessidade. Outra vantagem desse sistema, é a possibilidade de implementação de procedimentos e protocolos devidamente testados e avaliados impedindo que o investigador cometa erros que comprometam a investigação.

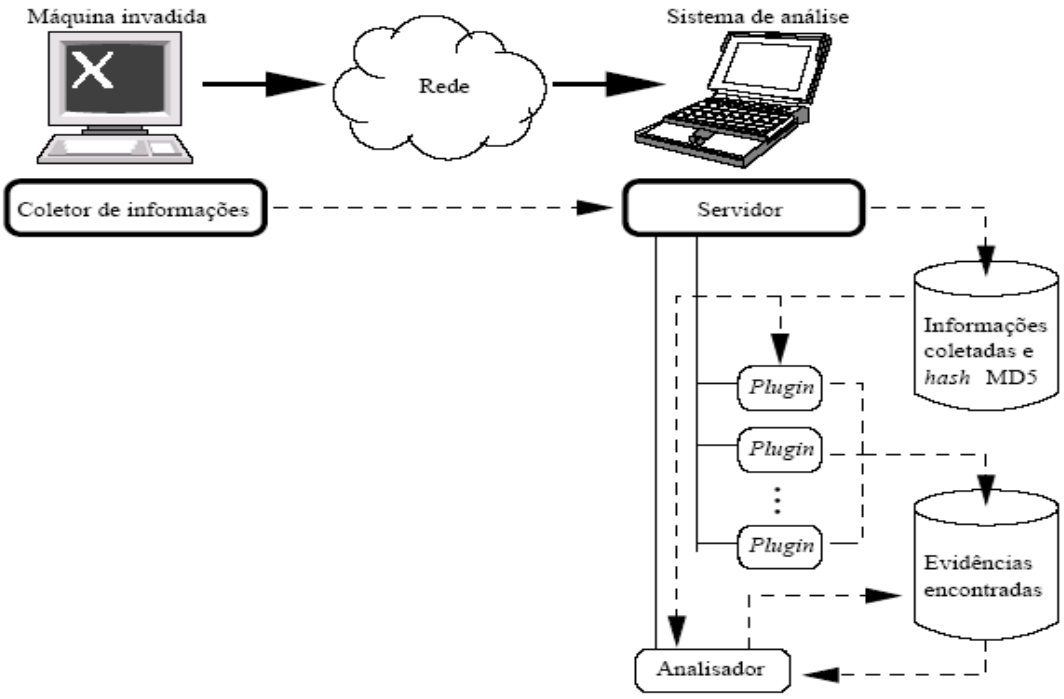

Figura 3 - Arquitectura extensível para um sistema automatizado de analise forense (Reis, 2003).

A figura 2, apresenta uma arquitectura extensível, para o desenvolvimento de um sistema automatizado de análise forense. A arquitectura é composta por um servidor designado que

representa um sistema de análise, e um cliente equipado de ferramentas para recolha de informações executado na máquina suspeita. O servidor neste caso é o componente principal, pois encarrega de receber as informações provenientes da máquina suspeita, organizá-las devidamente no sistema de análise (servidor), buscar as evidencias e analisá-las. O cliente é responsável pela recolha de informação na máquina invadida enviando-as para o servidor através da rede. Os plugins são responsáveis para a busca e extracção de evidências, por isso, cada um deles deve ser configurado com um conjunto de possíveis evidências que deverão ser procuradas. Em relação ao hashes criptografados, estes são gerados no momento da recolha de informação na máquina analisada, sendo enviados para o sistema de análise, juntamente com os dados recolhidos. O analisador é o responsável pela análise das evidências encontradas pelo plugins.

Para terminar, é importante ressaltar que durante as fases de análise deve-se documentar os procedimentos, isto é, a elaboração e documentação dos procedimentos a serem executados durante um incidente, inclusive referentes à investigação das máquinas afectadas, é essencial para a credibilidade e rapidez da resposta.

Apresentação

De acordo com Freitas (2006) apud Vargas (2007), esta fase é tecnicamente chamada de "substanciação da evidência", pois nela consiste o enquadramento das evidências dentro do formato jurídico, sendo inseridas, pelo juiz ou pelos advogados, na esfera civil ou criminal ou mesmo em ambas.

Desta forma, segundo Vargas, quando se tem a certeza material das evidências, actua-se em conjunto com uma das partes acima descritas para a apresentação das mesmas.

Ainda, segundo o mesmo autor, o investigador precisa estar perfeitamente sintonizado com os objectivos de cada etapa metodológica apresentada na secção 6.1, para poder minimizar o tempo e a quantidade de dados que deve obter até apresentar, maximizando sua eficiência e eficácia.

1.3.3 Fonte das evidências

Na concepção de Vargas (2007), a busca de indícios em um sistema computacional inicia-se com uma varredura minuciosa das informações nele contidas, seja em arquivos ou em memória, dados "deletados" ou não, cifrados ou possivelmente danificados.

Nas palavras de (Chaves, 2004), "…" "*A maior dificuldade no combate às condutas no meio electrónico é quando estas são praticadas por grandes profissionais. Estes costumam não deixar vestígios, utilizando-se de artimanhas de enganar a policia e dificultar a actuação dos peritos na sua identificação*.[5]"

Dispositivos de armazenamento da CPU

De acordo com Castro Jr et all (S/D), as informações contidas nos registradores de uma CPU embora são de mínima utilidade e sua captura é impraticável, podem conter informações que ainda não foram actualizadas na memória principal do sistema. Estes dados não possuem nenhum valor de prova pericial por conter apenas cálculos em linguagem de máquina impossíveis de serem traduzidos em informações com garantias.

Memória de periféricos

Geralmente, quase todos os dispositivos, conectados ou não, em um computador, podem conter memória, sendo esta de carácter temporário ou não. Como por exemplo,no caso das caixas automáticas, existem um conjunto de periféricos como (Dispensador de notas, impressora de recibos, leitor de cartões, etc) todos conectados a um computador podem conter em sua memória informações importantes a serem investigadas.

Memória principal do sistema

Embora, a perícia forense em sistemas computacionais é mais comummente realizada em discos rígidos e outros dispositivos de armazenamento não volátil as evidências podem também ser encontradas em memória principal.

[5] Disponível em: http://ceae.geness.ufsc.br/index.php?option=com_docman&task=doc_details&gid=592. Acessado em 16/09/2010.

Arquivos temporários (temp)

De acordo com Freitas (2006) apud Vargas (2007), alguns programas de processamento, desde o de texto até os que manipulam base de dados, criam arquivos temporários nos directórios durante sua execução. Esses arquivos são apagados automaticamente ao final da sessão de trabalho e como podem conter indícios de actos ilícitos deverão ser investigados.

Sector de swap

Segundo Freitas (2006)apud Vargas (2007), o gestor de memória do sistema operacional utiliza o sector de swap como uma grande área de armazenamento temporário de arquivos, que pode ser descarregados momentaneamente na memória principal, podendo ser tanto um arquivo quanto uma partição inteira do disco. Logo, este sector poderá conter alguma prova de algum acto ilícito, pelo que deve ser também investigada.

Sector de boot

Este sector trabalha na inicialização do sistema operacional, sendo possível, se modificado, carregar qualquer outro tipo de programa durante a inicialização do computador, de acordo com Freitas (2006) apud Vargas (2007). Exemplo: inserção de uma instrução no boot que irá inicializar algum tipo de ocorrência maliciosa no sistema operacional. Logo é importante também para o investigador a análise do sector de boot do computador periciado.

Sistemas de arquivos

Os arquivos de dados e executáveis representam a maior fonte de informação para o exame forense e são analisados para se determinar seu conteúdo e funcionalidade no sistema computacional. Estes podem ser procuradospor palavras-chave, imagens, dados específicos ou programas utilizados para práticas ilícitas Vargas (2007).

Segundo o mesmo autor, além de alterações, exclusão ou até mesmo inclusão de modificações inesperadas em directórios, arquivos (especialmente aqueles cujo acesso é restrito) podem

caracterizar-se como indícios para uma infracção. Exemplo: arquivos do tipo doc, txt, imagens, programas executáveis, aplicações instaladas (exe), dentre outras.

Arquivos de Logs

De acordo com Vargas (2007), os arquivos de logs também representam um papel importante na análise do sistema de arquivos, pois permitem a reconstituição de factos que ocorreram no sistema computacional, podendo registar entre outras informações as actividades dos utilizadores, dos processos e do sistema, as conexões e actividades de rede, podendo variar de acordo com o sistema operacional e serviços utilizados.

Ainda segundo Vargas, este serve para a indicação de acções em um determinado sistema operacional ou de alguma aplicação.

1.3.4 Perfil e métodos de operação do atacante

Segundo dados estatísticos sobre a criminalidade informática em Portugal, divulgados por representantes da Polícia Judiciária durante um evento, demonstra que o criminoso informático português tem entre 15 e 40 anos, é geralmente muito introvertido, cerca de metade é filho de pais separados/divorciados, frequenta o ensino superior numa vertente tecnológica, tira notas medianas e não tem antecedentes criminais.(fonte: http://www.miudossegurosna.net/artigos/2005-03-18-acapital.html)

Por outro lado, entender a motivação e o comportamento de um atacante segundo Reis & Geus (2002), é um ponto-chave para orientar a investigação, pois, essa compreensão fornece pistas sobre onde, como e o quê procurar durante a analise forense. Quanto maior a consciência acerca dos objectivos e métodos de operação de um atacante, maior o preparo do investigador para analisar e responder a um incidente.

Para Reis e Geus, a invasão de sistemas computacionais, ocorre com finalidades diversas, podendo ser destacada as seguintes:

- Obtenção de informações (roubo de segredos, números de cartões de credito, senhas e outros dados relevantes ao intruso);
- Promover algum estrago (destruição de informações e paralisação do sistema, por exemplo);
- Utilização dos recursos do sistema (repositório de dados, disseminação de ataques distribuídos, provimento de serviços, por exemplo);

Dependendo da finalidade e da habilidade, o método de operação de um invasor pode sofrer algumas variações. Entretanto, os passos tomados pelo atacante para comprometer um sistema computacional podem ser generalizados como se segue:

- Identificação do alvo;
- Busca de vulnerabilidades no alvo;
- Comprometimento inicial;
- Aumento de privilégio;
- Tornar-se "invisível;
- Reconhecimento do sistema;
- Instalação de backdoors;
- Limpeza de rastos e por fim;
- Fazer retorno através de backdoor.

Para os mesmos autores, a primeira atitude do atacante é a escolha de um alvo potencial. Uma vez localizado, o atacante começa a reunir informações sobre o sistema a fim de identificar vulnerabilidades no sistema operacional ou serviços de rede disponíveis. Se um invasor ainda não possui uma combinação de senha valida para o sistema, ele utiliza métodos como snifing e adivinhação de senhas, engenharia social ou scanning para encontrar um ponto de entrada. Uma vez encontrado, o invasor realiza o comprometimento inicial do sistema.

A primeira intrusão geralmente provoca muito "barulho", principalmente se o sistema alvo estiver devidamente equipado, por isso a intrusão costuma ocorrer quando ninguém está presente para ouvir.

Depois que o atacante ganha acesso ao sistema, busca privilégio irrestritos (conta de administrador ou root) e para o efeito, transfere programas maliciosos (conhecidos por exploits). Quando o invasor obtém acesso de root e garantir a sua "invisibilidade", procura saber o quanto a sua presença perturba o sistema invadido e, por conseguinte, se pode ser descoberta (analisando a configuração de log). Em seguida, ele investiga as medidas de segurança implementadas no sistema invadido. Em alguns casos, até corrige vulnerabilidades existentes para impedir que outro invasor faça uso do sistema.

Após compreender as configurações do sistema, o atacante instala backdoors para facilitar seu retorno e paga os rastos deixados por sua presença no sistema. Utilizando uma backdoor, oinvasor retorna de forma mais discreta que o comprometimento inicial e faz um inventário acerca das informações existentes na máquina invadida e dos potenciais alvos de vizinhança.

Ainda, segundo (Reis & Geus, 2002), a habilidade do invasor em executar o método de operação descrito anteriormente pode ser fundamental para o processo de análise forense, pois a quantidade de evidências deixadas depende directamente do nível de conhecimento do atacante.

Para ilustrar essa relação, é possível classificar a habilidade de invasor em quatro classe, de acordo com: Clueless, script Kiddie, Guru e Wizard. A tabela 1 apresenta a relação entre a habilidade do invasor e a quantidade de evidências deixadas.

Nível de habilidade	Habilidades	Evidências
Clueless	Nenhuma habilidade	Todas as evidências são bastantes aparentes
Script Kiddie	Capaz de encontrar exploits prontos na Internet e executá-los seguindo intrusões detalhadas. Não escrevem programas	Pode tentar cobrir rastos com o uso de rootkits prontos, mas com sucesso limitado. Pode ser detectado com esforço mínimo
Guru	Equivalente a um administrador	Cuidadosamente apaga evidências em

	experiente. Hábil em programação. Checa a existência de programas de segurança e esquemas de log seguros, evitando alvos protegidos	arquivos de log. Não deixa traços óbvios de sua presença. Pode instalar trojan horses e backdoors para um acesso futuro
Wizard	Possui um grande conhecimento do funcionamento interno de um sistema. Capaz de manipular hardware e software	Praticamente não deixa evidências úteis. Pode comprometer totalmente o sistema

Tabela 2:Relação entre a habilidade do invasor e a quantidade de evidência deixadas

Fonte: (Reis & Geus, 2002)

1.4 Técnicas anti-forense

Se por um lado a forense computacional procura por vestígios de acções criminosa ocorrida, as técnicas anti-forense faz o oposto, ou seja, ela diz respeito a qualquer estratégia de eliminação de informação que possa ser usada em um processo de análise forense.(Bueno, 2007)

1.4.1 Identificação da autoria

A identificação da autoria, quando efectuada nos meios electrónicos, torna-se motivo de grande preocupação sobretudo para os especialistas em novas tecnologias.

A maior dificuldade no combate aos crimes conduzidos em meios electrónicos é quando os mesmos são praticados por profissionais de grande conhecimento. Tais profissionais costumam não deixar vestígios, utilizando técnicas com objectivo de enganar a policia e deste modo dificultar a actuação dos peritos na sua identificação Também, por outro lado porque os criminosos na internet, os chamados crackers estão cada vez mais actualizados em matéria de novas tecnologia, o que dificulta as empresas na prevenção das suas politicas de segurança e dos sistemas informáticos. (Chaves, 2004)

Ainda, de acordo com (Chaves, 2004), um outro motivo que dificulta o combate às condutas no meio electrónico é quando estes profissionais utilizam computadores de terceiros para praticarem crimes. Logo será difícil aos especialistas, implementarem politica de combates. Através do endereço IP utilizados, registo de log de acesso, conta de e-mail, cadastros nos provedores e sites já é possível a identificação da autoria.

Entretanto, a identificação da autoria apresenta um grande problema: Em primeiro lugar porque encontrar a máquina evolvida no crime não quer dizer que encontrado o autor do crime.

1.4.2 Criptografia

Segundo Bueno (2007), se por um lado a criptografia fornece um nível de segurança às informações, por meios de cifragem de dados, ela pode também ser usada para cifrar dados comprometedores para evitar o cesso ao seu conteúdo. Isso pode representar ser uma grande dificuldade para a forense na sua decifragem.

1.4.3 Esteganografia

Diferentemente da criptografia, que busca cifrar o conteúdo de uma informação mascarando o real conteúdo, a esteganografia busca ocultar a existência de uma informação. Para fazer tal efeito, é usado um objecto para conter essa informação que se pretende esconder. A ocultação é feita de tal modo que apenas o destinatário e o remetente devem ser capaz de verificar sua existência. (Bueno, 2007)

2 Servidor Web – Microsoft IIS

Segundo (Freitas, 2006), os ataques com base em Web geralmente se encaixam em três categorias: ataques contra o próprio servidor (DoS e DDoS), ataques contra o conteúdo do site (desfiguração de site, também conhecido como defacement) e ataques contra a empresa (roubo de produto ou informação).

Para Freitas (2003), os ataques via web são frequentes devido à vulnerabilidade de software e autenticação do sistema operacional e os mais comuns são os de desfiguração de site.

Para este mesmo autor, num incidente de segurança, diversos arquivos de logs podem ser usados para confirmar ou não se um incidente ocorreu e então determinar o tipo, extensão, causa e origem do incidente. Somente uma entrada no arquivo de log possa não ser suficiente para termos uma imagem do incidente. Será necessário um conjunto de entrada para dar o investigador um controle de tempo e o contexto necessário para compreender o referido incidente.

2.1 Microsoft IIS

O Microsoft IIS (Internet Information Service) é o servidor web da Microsoft, considerado o segundo servidor web mais usado do mundo, a seguir ao Apache.

Segundo (Freitas, 2006), trata-se de um servidor de Internet/Intranet dos sistemas operacionais Windows. A primeira versão do IIS foi disponibilizada em 1996 e hoje, na versão 6, o IIS se encontra mais estável, seguro e integrado ao sistema operacional.

Existem várias versões disponível no mercado no qual se destaca:

Microsoft IIS 1.0, Windows NT 3.51;

Microsoft IIS 2.0, Windows NT 4.0;

Microsoft IIS 3.0, Windows NT 4.0 Service Pack 3;

Microsoft IIS 4.0, Windows NT 4.0 Option Pack;

Microsoft IIS 5.0, Windows 2000;

Microsoft IIS 5.1, Windows XP Professional, Windows XP Media Center Edition;

Microsoft IIS 6.0, Windows Server 2003 and Windows XP Professional x64 Edition;

Microsoft IIS 7.0, Windows Server 2008 e Windows Vista (Home Premium, Business, Enterprise, Ultimate Editions);

Microsoft IIS 7.5, Windows Server 2008 R2 e Windows 7;

Normalmente, os campos mais importantes para investigar os incidentes suspeitos são o registo data/hora, endereço IP de origem, código do status do HTTP e recursos requisitados.

2.1.1 História e evolução

IIS 1 – Internet Information Server 1

Segundo (Freitas, 2006) esta é a primeira versão o Microsoft IIS, liberada em Fevereiro de 1996 como um add-on do Windows NT 3.51. Este suportava os três principais protocolos da Internet: HTTP, TFP e Gopher.

O Microsoft IIS 1 apresenta algumas características como: (Freitas, 2006)

- Internet Service Manager (ferramenta para gerenciamento do IIS);
- Integração com o sistema operacional Windows NT 3.51;
- Servidores Virtuais;
- Directórios Virtuais;
- ISAPI (Internet Server API);
- Autenticações Basic e NTLM (Windows NT LAN Manager);
- SSL (Secure Sockets Layer);
- IDC (Internet Database Connector);
- Arquivos de Log nos formatos texto e ODBC.

IIS 2 – Internet Information Server 2

Uma das mudanças desta versão em relação a versão anterior foi o facto do IIS 2 se tornar parte da instalação do Windows NT 4, e os principais itens incluído no IIS2 foram os seguintes, segundo (Freitas, 2006):

- IDQ (Internet Data Query);
- HTX (Hipertext Extension);

- Possibilidade de administrar o IIS através de um browser;
- Key Manager;
- Index Server;
- Nova versão do Internet Service Manager.

Na instalação do IIS 2, o Windows NT 4 cria uma conta de usuário específico para acesso anónimo ao servidor web chamada de IUSR_nomecomputador. Relativamente a estrutura dos directórios, são criados e utilizados pelo IIS 2 os seguintes directórios: (Freitas, 2006)

- [Driver]:\Winnt\System32\InetSrv – Neste directório ficam as DLLs, executáveis, arquivos e scripts necessários para administrar o IIS via browser, documentação do IIS etc.;
- [Driver]:\ Winnt\System32\LogFiles – Local onde estão armazenados os arquivos de logs;
- [Driver]:\InetPub – Por padrão, é onde ficam armazenadas as aplicações web.

Para este mesmo autor, o formato de arquivos de logssuportados pelo IIS 2 são:

- NCSA Common Log File Format;
- Formato padrão;
- E Log ODBC.

IIS 3 – Internet Information Server 3

Quando o Service Pack 3 do Windows NT 4 era instalado, o IIS 2 recebia uma actualização para a versão 3. Esta actualização foi disponibilizada em Dezembro de 1996 (a terceira versão do IIS em menos de um ano). Com esta versão o IIS começou a ser reconhecido não apenas como um servidor web, mas também como uma plataforma de desenvolvimento. Algumas das novas características implementadas no IIS 3 são, de acordo com (Freitas, 2006):

- Desenvolvimento Web com ASP, VBScript, Jscript, ADO, ActiveX e ODBC;
- Suporte ao MTS (Microsoft Transaction Server);
- Suporte ao Microsoft Frontpage 97 Server Extension;
- Suporte ao Microsoft NetShow (streaming de ádio e vídeo);

- Suporte ao Visual interDev (Desenvolvimento de aplicações Web).

Segundo o mesmo autor, na instalação do IIS 3, é criada no Sistema Operacional Windows NT 4 uma conta de utilizador específica para o acesso anónimo ao servidor web chamada de IUSR_nomedocomputador e os logs suportados pelo IIS 3 são:

- Microsoft IIS Log File Format;
- NCSA Common Log File Format;
- W3C Extended Log File Format;
- Log ODBC.

IIS 4 – Internet Information Server 4

O IIS 4 foi disponibilizado em Março de 1998 como um componente do Option Pack do Windows NT 4. Com o Option Pack, a Microsoft tentava fazer do windows NT 4 uma plataforma mais segura e confiável, pois a cada dia o Windows NT avançava mais nas estatísticas do mercado e o IIS 4 foi o mais significativo upgrade de versão até então. Alguma das características incluídas no IIS 4, segundo (Freitas, 2006) são:

- O Internet Service Manager deu lugar ao Microsoft Management Console (MMC);
- HTTP versão 1.1;
- SSL (Secure Sockets Layer) versão 3;
- Metabase;
- SMTP (Simple Mail Transport Protocol);
- NNTP (Network News Transport Protocol).

De acordo com este mesmo autor, na instalação do IIS 4 são criadas duas novas contas de utilizadores no sistema operacional Windows NT 4: IUSR_nomedocomputador (conta interna para acesso anónimo ao IIS) e o IWAM_nomedocomputador (conta interna para o IIS iniciar a partir de aplicativos de processo). Esta versão do IIS, suporta os seguintes arquivos de log:

- Microsoft IIS Log File Format;
- NCSA Common Log File Format;
- W3C Extended Log File Format;

- Log ODBC.

IIS 5 – Internet Information Services 5

Segundo (Freitas, 2006), o IIS5 foi liberado como parte do Sistema Operacional Windows 2000 Server dois anos mais tarde. Uma das diferenças entre as versões 4 e 5 foi a mudança do nome de "Internet Information Server" para "Internet Information Serveces". As novas caracteristicas incluídas no IIS 5 foram:

- Utilização de processos em Pool;
- Controle do tempo da CPU;
- Integração com o Active Directory;
- Novos Wizards;
- Suporte ao WebDAV (Web Distributed Authoring and Versioning).

Na instalação do IIS 5, segundo Freitas, são criadas duas novas contas de utilizadores no Sistema Operacional Windows 2000 e os arquivos de logs suportados são os mesmos que IIS 4.

IIS 6 – Internet Information Services 6

O Microsoft IIS 6 é disponibilizado como um add-on do Sistema Operacional Windows Server 2003 e representa uma mudança fundamental nos produtos Web oferecidos pela Microsoft. As novas características incluídas no IIS 6 são:

- Nova arquitectura;
- Várias recursos e tecnologias de segurança;
- Várias ferramentas de gerenciamento e administração;
- Maior integração com o .NET.

Na instalação do IIS 6 são criados duas novas contas de utilizadores e um novo grupo no Sistema Operacional Windows que segundo Freitas são:

Utilizador: IUSR_nomedocomputador (conta interna para acesso anónimo ao IIS) e IWAM_nomedocomputador (conta interna para o IIS iniciar a partir de aplicativos de processos. Membro do grupo IIS_WPG).

Grupo: IIS_WPG (O grupo IIS_WPG é criado para simplificar o processo de configuração de autorizações).

Relativamente aos arquivos de logs, o IIS suporta (Freitas, 2006):

- Microsoft IIS Log File Format;
- NCSA Common Log File Format;
- W3C Extended Log File Format;
- Log ODBC;
- Log Binário Centralizado.

IIS 7 – Internet Information Services 7

Os Serviços de Informação Internet (IIS) 7 desempenham a função Web Server (IIS) no Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista.

O IIS 7.0 divide o servidor Web em um servidor principal leve e em mais de 40 módulos de recursos que podem ser conectados neste servidor principal. Esses módulos – como o staticFileModule, que permite o download de conteúdo estático da web, ou o WindowsAuthModule, que aceita autenticação NTLM integrada – podem ser instaladas independentemente no servidor para oferecer a funcionalidade exacta precisada. (fonte:http://msdn.microsoft.com/pt-br/magazine/cc163453.aspx)

De acordo com a mesma fonte, no servidor IIS 7 pode ser adicionado as seguintes extensões:

Extensões IIS	Descrição
Serviço de Publicação FTP	O Serviço de Publicação de FTP para IIS 7 permite que os criadores de conteúdo da Web publiquem conteúdo mais seguramente para servidores da web do IIS 7 com novos recursos como autenticação com base em SSL e transferência de dados. Para obter mais informações, consulte Administering FTP 7.5.
Pacote de Administração	O Pacote de Administração do IIS 7 adiciona aos recursos de gerenciamento no IIS 7 para incluir o suporte de UI de administração para autorização de ASP.NET, erros de personalização, configuração de FastCGI, Filtragem de Solicitação e mais. Para obter mais informações, consulte a Ajuda da Interface de Usuário do Administration Pack.
Roteamento de Solicitação do Aplicativo	Roteamento da Solicitação do Aplicativo (ARR) da Microsoft para IIS 7 é um módulo de roteamento com base em proxy que encaminha as solicitações de HTTP para servidores de conteúdo com base em leitores de HTTP, variáveis de servidor e algoritmos de balanço de carga. Para obter mais informações, consulte a Application Request Routing User Interface (UI) Help.
Gerenciador de Banco de Dados	O Gerenciador do Banco de Dados do IIS permite o fácil gerenciamento de bancos de dados remotos e locais de dentro do Gerenciador do IIS. O Gerenciador de Banco de Dados do IIS também descobre automaticamente bancos de dados com base no servidor da web ou configurações do aplicativo e fornece a habilidade de se conectar com qualquer banco de dados na rede. Para obter mais informações, consulte a IIS Database Manager User Interface (UI) Help.
Módulo de Regravação de URL	O módulo de regravação de URL fornece um mecanismo de regravação com base em regra para alterar os URLs de solicitação antes que eles sejam processados pelo servidor da web. O módulo pode ser usado para expressar a lógica de regravação de URL que pode usar expressões normais ou curingas e para tomar decisões de regravação com base em cabeçalhos de HTTP e variáveis de servidor. Para obter mais informações, consulte a IIS URL Rewrite Module.

WebDAV	A Extensão WebDAV para IIS 7 permite que autores da web publiquem conteúdo com mais segurança para servidores da web do IIS 7 e permite que administradores da web e hosters gerenciem configurações WebDAV usando as ferramentas de gerenciamento e configuração de IIS 7. Para obter mais informações, consulte WebDAV.
Ferramenta de Implantação da Web	A Ferramenta de Implantação da Web simplifica a migração, o gerenciamento e a implantação de servidores da web, aplicativos e locais IIS. Ela permite que administradores e usuários delegados sincronizem o IIS 6.0 e servidores do IIS 7, migrem um servidor IIS 6.0 para IIS 7 e implantem aplicativos da web em um servidor IIS 7. Para obter mais informações, consulte Web Deployment Tool.

Tabela 3: Extensões do IIS 7 (Microsoft, 2007)

IIS 7.5 – Internet Information Services 7.5

Segundo a Microsoft[6], os Serviços de Informação Internet (IIS) 7.5 desempenham a função Web Server (IIS) no Windows Server® 2008 R2 e o servidor Web no Windows® 7. O servidor Web foi reestruturado no IIS 7 para permitir a personalização de um servidor, através da adição ou remoção de módulos, com vista a satisfazer as suas necessidades específicas. Os módulos são funcionalidades individuais que o servidor utiliza para processar pedidos. Por exemplo, o IIS utiliza módulos de autenticação para autenticar credenciais de cliente e módulos de cache para gerir a actividade da cache.O IIS 7.5 possui as seguintes funcionalidades:

ASP.NET

O ASP.NET fornece um ambiente de programação orientada para objectos do lado do servidor para a criação de Web sites e aplicações Web que utilizam código gerido. O

[6] Disponível em: http://technet.microsoft.com/pt-pt/library/cc753473%28WS.10%29.aspx. Acessado em 20/09/2010.

ASP.NET não é apenas uma nova versão do ASP. O ASP.NET fornece uma infra-estrutura robusta para a criação de aplicações Web e foi completamente remodelado para proporcionar uma experiência de programação altamente produtiva baseada no .NET Framework.

Extensibilidade .NET

A Extensibilidade .NET permite aos programadores de código gerido alterar, adicionar e expandir a funcionalidade do servidor Web no pipeline de pedidos, na configuração e na IU. Os programadores podem utilizar o modelo de extensibilidade do ASP.NET conhecido e as APIs avançadas do .NET para criar funcionalidades do servidor Web tão eficazes quanto as escritas através das APIs de C++ nativas.

ASP

O Active Server Pages (ASP) fornece um ambiente de scripts do lado do servidor para a criação de Web sites e aplicações Web. O ASP oferece um desempenho melhorado em relação aos scripts CGI ao dotar o IIS de suporte nativo tanto para VBScript como para JScript. Utilize o ASP se tiver aplicações existentes que necessitem de suporte ASP. Para novos desenvolvimentos, considere utilizar o ASP.NET.

CGI

A Common Gateway Interface (CGI) define o modo como um servidor Web transmite informações a um programa externo. As utilizações habituais podem incluir a utilização de um formulário Web para recolher informações e, em seguida, transmitir essas informações a um script CGI para ser enviado por correio electrónico para outro local. O facto de a CGI ser um padrão faz com que os scripts CGI possam ser escritos utilizando várias linguagens de programação. A desvantagem de utilizar a CGI está na sobrecarga de desempenho.

Extensões ISAPI

As extensões ISAPI (Internet Server Application Programming Interface) fornecem suporte ao desenvolvimento de conteúdo Web dinâmico utilizando extensões ISAPI. Uma extensão ISAPI é executada mediante pedido, tal como qualquer outro ficheiro HTML estático ou ficheiro ASP dinâmico. Como as aplicações ISAPI são código compilado, são processadas

muito mais rapidamente do que os ficheiros ASP ou ficheiros que chamam componentes COM+.

Filtros de ISAPI

Os Filtros Internet Server Application Programming Interface (ISAPI) fornecem suporte às aplicações Web que utilizam filtros ISAPI. Os filtros ISAPI são ficheiros que podem expandir ou alterar a funcionalidade fornecida pelo IIS. Um filtro ISAPI analisa cada um dos pedidos efectuados ao servidor Web até encontrar um que necessite de ser processado.

Server-Side Includes

O SSI (Server Side Includes) é uma linguagem de scripts utilizada para gerar páginas HTML de forma dinâmica. O script é executado no servidor antes de a página ser entregue ao cliente e envolve, habitualmente, a inserção de um ficheiro noutro. Por exemplo, pode criar um menu de navegação HTML e utilizar o SSI para adicioná-lo dinamicamente a todas as páginas de um Web site.

2.2 Arquitectura

O IIS implementa 5 serviços básico para a publicação na internet que segundo (Júnior, 2007) são:

- WWW, que oferece a publicação aos utilizadores finais do IIS, através do HTTP cliente;
- FTP, que oferece a transferência e o gerenciamento de pacotes;
- SMTP, protocolo que é utilizado para enviar e-mails, podendo programar os servidores para envio de e-mails relacionados a eventos bem ou mal sucedidos;
- NNTP, que é o protocolo de notícias, podendo assim qualquer utilizador utilizando qualquer leitor de notícias cliente, verificar as noticias daquele grupo;

- E o serviço de administração, que mantém o registo do Windows actualizado para os serviços citados acima e gerência a metabase do IIS. A metabase é um armazenamento de dados onde ficam guardados todos as configurações do IIS.

2.3 Arquivos de Log

A forma mais simples de segurança de um web site é manter um log dos computadores que contactam o site. O log é um registo de quem visitou, quando visitou e o que procurou no site. Nestes mesmos logs, pode-se descobrir quantas pessoas estão a usar o site e se alguém está fazendo mau uso deste.Os arquivos de logs padrão encontra-se localizado no directório C:\Winnt\System32\Logfiles\W3SVC1 e o nome do log é baseado na data actual, no formato exaammdd.log, por exemplo: 010910.log . O formato padrão é W3C (World Wide Web Consortium) Extended Log File Format (Formato de Arquivo de Log Extendiso), um formato padrão que muitos utilitários de terceiros interprestam e analisam. Outros formatos disponíveis são: Microsoft IIS Log File Format (Formato de Log do Microsoft IIS), NCSA Common Log File Format (Formato de arquivo de Log comum do NCSA) e Log do ODBC (Open Database connectivity), em sistemas Windows 2000, que envia um formato fixo á uma base de dados específico. (Freitas, 2006)

Nesta perspectiva, os arquivos de logs podem ser usados para confirmar ou não se uma invasão ocorreu em um sistema e desta forma determinar o tipo, extensão causa e origem do incidente.

2.3.1 W3C Extended Log File Format

O formato estendido do W3C, como mostra a figura abaixo, é um formato ASCII personalizável com vários campos diferentes. Desta forma, pode ser incluído campos importantes, limitando o tamanho do log e omitindo campos indesejáveis. Os campos são separados por espaços e o horário registado como UTC (horário de Greenwich). (Freitas, 2006)

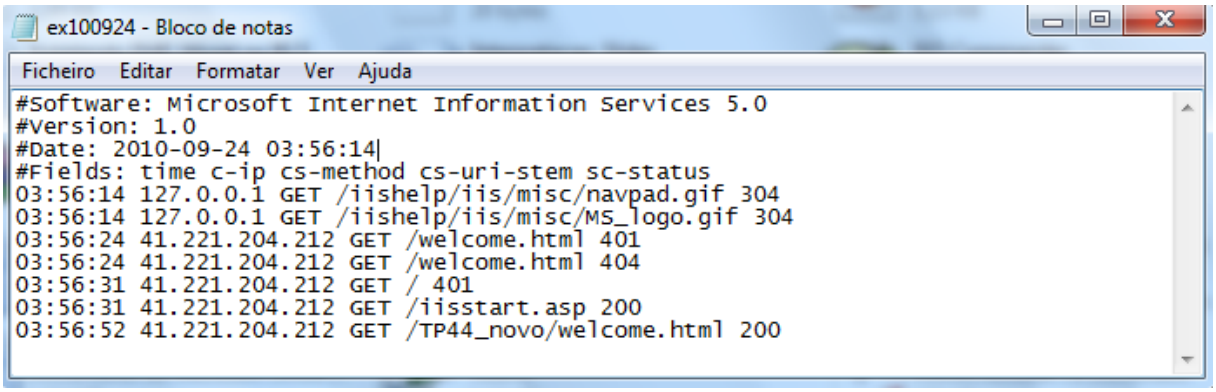

Figura 4 - Exemplo de um W3C Extended Log File Format

Definições do Log do W3C Extended Log Fife Format

CAMPO	APARECE COMO	DESCRIÇÃO
Data	date	Data de ocorrência da actividade.
Hora	time	Hora de ocorrência da actividade.
Endereço IP do cliente	c-ip	Endereço IP do cliente que acessou o servidor.
Nome do utitlizador	cs-username	Nome do utilizador autenticado que acessou o servidor. Isst não inclui utilizadores anônimos, representado por um hifen.
Nome do serviço e número da instância	s-sitename	O servivo de internet e o número da instância executados no PC cliente.
Nome do servidor	s-computername	Nome do Servidor em que a entrada de log foi gerada.
IP do servidor	s-ip	Endereço IP do servidor em que a entrada de log foi gerada.
Método	cs-method	Acção que o cliente estava tentando executar (por exemplo, um método GET).
Tronco URI	cs-uri-stem	Recurso acessado (por exemplo, o Default.html).
Consula URI	cs-uri-query	A consulta (se houver), que o cliente estava tentando fazer.
Status do http	sc-status	Status da acção, nos termos empregados pelo http.
Status do Win32	sc-win32-status	Status da acção, nos termos empregados pelo windows 2000.
Bytes enviados	sc-bytes	Número de bytes enviado pelo servidor.

Bytes recebidos	cs-bytes	Número de bytes recebido pelo servidor.
Porta do servidor	s-port	Número da porta a qual o cliente está conectado.
Tempo gasto	time-taken	Tempo gasto durante a acção.
Versão do protocolo	cs-version	Versão do protocolo (HTTP, FTP) utilizada pelo cliente. No caso do HTTP, será HTTP 1.0 ou HTTP 1.1.
Agente do utilizador	cs(user-agent)	Navegador utilizado no cliente.
Cookie	sc(cookie)	Conteúdo do cookie enviado ou recebido, se houver.
Referenciador	sc(referer)	Site anterior visitado pelo utilizador. Este site fornece um link para o site actual.

Tabela 4: Definições do Log do W3C Extended Log File Format – (Freitas, 2006)

Segundo (Freitas, 2006), os prefixos usados na tabela acima, apresentam os seguintes significados:

s-: Acções do servidor;

c-:Acções do cliente;

cs-:Acções de cliente para servidor;

sc-:Acções de servidor para cliente.

Definições do Log de Contabilização de Processo

CAMPO	APARECE COMO	DESCRIÇÃO
Tipo de processo	s-process-type	Tipo de processo disparado pelo evento, um aplicativo CGI ou fora de processo. O tipo pode ser CGI, Aplicativo ou Todos.
Evento de processo	s-event	O evento disparado: Site-stop, site-start, site-pause, periodic-log, interval-start, interval-change, log-change-int/start/stop, eventlog-limit, priority-limit, process-stop-limit, site-pause-limite, eventlog-limit-reset, priority-limite-reset, process-stop-limit-reset ou site-pause-limit-reset.

Tempo total do utilizador	c-user-time	Tempo total acumulado do processador de modo do utilizador, em segundos, utilizado pelo site durante o intervalo actual.
Tempo total do núcleo	s-kernel-time	Tempo total acumulado do processador de modo do núcleo, em segundos utilizado pelo site durante o intervalo actual.
Tempo de falhas da página	s-page-faults	Núcleo total de referência de memória que resultou em falhas de página de memória.
Total de processos	s-total-procs	Núcleo total de aplicativos CGI e fora de processo, criados durante o intervalo actual.
Processos activos	s-active-procs	Núcleo total de aplicativos CGI e fora de processo em execução quando o log foi gravado.
Total de procssos encerrados	s-topped-procs	Núcleo total de aplicativos CGI e fora de processo parado devido ao estreitamento do processo, durante o intervalo actual.

Tabela 5: Definições de Log de Contabilização de Processos (Freiras, 2006)

Freitas, apresenta para cada valor referido acima, o seguinte significado:

Site-stop: Site da web parado por algum motivo;

Site-start: Site da web iniciado ou reiniciado;

Site-pause: Pausa no site da web;

Periodic-Log: Entrada de log definida regularmente, cujo intervalo foi especificado pelo administrador;

Interval-start: Intervalo de redefinição iniciado;

Interval-End: Intervalo de redefinição atingido e redefinido;

Interval-change: O administrador do site da web alterou o valor do intervalo de redefinição;

Log.change-int/start/stop: Ocorreu um dos seguintes eventos: intervalo de log modificado; evento de intervalo; ou site parado, iniciado ou interrompido;

Eventlog-limit: Log de evento criado para site da web porque um aplicativo CGI ou fora de processo atingiu o limite de log de evento definido pelo administrador;

Priority-limit: O site da web teve um aplicativo CGI ou fora de processo definido com baixa prioridade porque atingiu o limite de baixa prioridade definido pelo administrador;

Process-stop-limit: O site da web teve um aplicativo CGI ou fora de processo parado porque atingiu o limite de paralisação de processos definido pelo administrador;

Site-pause-limite: O site da web foi interrupção de sites definido pelo administrador;

Eventlog-limit-reset: O intervalo de redefinição foi alcançado ou o Eventlog-limit foi redefinido manualmente;

Priority-Limit-reset: O intervalo de redefinição foi alcançado ou o Priority-limit foi redefinido manualmente;

Process-stop-limit-reset: O intervalo de redefinição foi alcançado ou o Process-stop-limit foi redefinido manualmente;

Site-pause-limit-reset: O intervalo de redefinição foi alcançado ou o site-pause-limit foi redefinido manualmente.

De todos os campo que podem ser encontrados nos arquivos de logs, o HHTP status (sc-status) requer alguma explicação. De uma forma geral, qualquer código entre 200 e 299 indica sucesso, os códigos entre 300 e 399 indicam acções que precisam ser tomadas pelo cliente para cumprir um pedido. Os códigos entre 400 e 499 e 500 e 599 indicam erro do cliente e servidor, respectivamente.

2.3.2 *Microsoft IIS Log File Format*

O formato de log Microsoft, tem uma grande diferença em relação ao formato W3C, pois não é personalizável, mas em compensação ele é mais completo que o formato NCSA. O facto de não ser personalizável, ele vem com alguns itens básicos, nomeadamente: IP e nome do utilizador, data e hora de solicitação, código de status do http e o número de bytes recebidos. Um outro aspecto muito importante a se levar em consideração é que os itens do formato Microsoft vêm separado por vírgula, tornando assim mais fácil a sua leitura.(Júnior, 2007)

2.3.3 *NCSA Common Log File Format*

O format NCSA é muito parecido com o formato Microsoft, pois também não é personalizável. Este, regista as informações básicascomo, nome do utilizador e do host remoto, a data, horário, o tipo de solicitação, o código de status do http e o número de bytes recebidos. Também este formato está disponível para sites da web e não para sites FTP. (Júnior, 2007)

2.3.4 *Log ODBC*

Segundo (Freitas, 2006), o log ODBC é uma outra opção de registar as solicitações do site em uma base de dados. Para incluir as informações em uma base de dados, será preciso configurar o DNS (Data Source Name, nome da fonte de dados), a tabela e especificar o nome do utilizador e a senha a serem usados durante o registo na base de dados.

Muito diferentemente das outras opções, o registo ODBC em uma única transmissão cria vários registos na base de dados. Por causa desse grande número de entradas, o registo do ODBC requer mais recursos do servidor do que os outros tipos de log, o que pode afectar o desempenho do servidor web, dependendo do tipo de base de dados, localização e quantidade de entradas registadas.(Freitas, 2006)

Ainda, para o mesmo autor, os registos ODBC geram os seguintes campos:

ClientHost	Endereço IP do cliente
Username	Nome de domínio do cliente
Logtime	Data e hora da conexão
Service	Serviço do Internet Information Server
Machine	Nome do computador
ServerIP	Endereço IP do servidor
Processing Time	Tempo de processamento em milissegundos
BytesRecvd	Bytes recebidos pelo servidor
BytesSent	Bytes enviados pelo servidor

ServiceStatus	Código de resposta do protocolo
Win32Status	Status do Windows 2000 Server ou o código de erro
Operation	Comando do protocolo
Target	Destinatário
Paramenters	Parâmetros

2.3.5 Log Binário Centralizado

O log binário centralizado encontra-se disponível apenas no IIS 6 (Windows 2003) e é um processo onde vários sites inserem dados sem formatação em um único arquivo do tipo binário. Normalmente, quando esse tipo de log for habilitado, o IIS cria um arquivo com a extensão.ibl. Por ser um arquivo binário, serão necessárias ferramentas específicas para compreender as informações do log. (Freitas, 2006)

2.3.6 Nomes de Arquivos de Log

Os nomes de arquivos usam as várias das primeiras letras para representar o formato de log e os números restantes para representar o intervalo de tempo ou a sequência do log. As letras em itálico representam dígitos tais como: *nn* para os dígitos sequenciais, *yy* para o ano, mm para o mês, *ww* para a semena do mês *dd* para o dia, *hh* para o horário no formato de 24 horas.

A tabela abaixo ilustra os nomes dos arquivos:

FORMATO	CRITÉRIO	PADRÃO DE NOME DE ARQUIVO
Formato de log Microsoft IIS	Por tamanho do arquivo	**inetsv***nn*.log
	Por hora	**in***yymmddhh*.log
	Diariamente	**in***yymmdd*.log

	Semanalmente	**in***yymmww*.log
	Mensalmente	**in***yymm*.log
Formato de arquivo de log comum do NCSA	Por tamanho do arquivo	**ncsa***nn*.log
	Por hora	**nc***yymmddhh*.log
	Diariamente	**nc***yymmdd*.log
	Semanalmente	**nc***yymmww*.log
	Mensalmente	**nc***yymm*.log
Formato de arquivo de log estendido do W3C	Por tamanho do arquivo	**extend***nn*.log
	Por hora	**ex***yymmddhh*.log
	Diariamente	**ex***yymmdd*.log
	Semanalmente	**ex***yymmww*.log
	Mensalmente	**ex***yymm*.log
Log binário centralizado	Por hora	**ra***yymmddhh*.ibl
	Diariamente	**ra***yymmdd*.ibl
	Semanalmente	**ra***yymmww*.ibl
	Mensalmente	**ra***yymm*.ibl

Tabela 6: Nome de arquivos de Log (Freitas, 2006)

3 Ferramentas Forense

Com o advento e disseminação da tecnologia nesses últimos anos, as infracções, invasões, venda e roubo de informações privilegiadas, pirataria, envio de e-mails falsos, tentativas de acessos indevidos à organizações ou até mesmo à pessoas comuns vêm se aumentando cada vez mais e por isso há a necessidade do auxílio de ferramentas mais modernos e incrementada para busca de infractores, além da necessidade de padronização das buscas e apresentação das evidências mais consistentes.(Vargas, 2006)

Neste sentido, será apresentado neste capítulo uma listagem de ferramentas mais comummente utilizado na investigação forense.

3.1 Forense na Web

Para facilitar o trabalho de buscas pelas pastas dentro do cache, pode-se usar algumas ferramentas que fornecem listagens de histórico e cache do IE, automatizando a tarefa de verificação manual de arquivos de índice e pastas de conteúdo. A título de exemplo cita-se: (Bueno, 2007).

Pasco: Trabalha sobre o arquivo do índice da cache. A sua saída é um arquivo de texto, contendo os registros encontrados. Pode ser usado para processar arquivos de índice de histórico desse navegador também.

Web Historian: Ferramenta que processa arquivos de histórico de IE e de outros navegadores também (Firefox, Opera e Safari). Permite a escolha de diversos formatos de saída, como, por exemplo, em uma planilha de Microsoft Excell, o que facilita a visualização dos resultados.

Forensec Tool Kit (FTK): Ferramenta que possui um navegador "embutido" para tornar imediata a associação entre registo do item de cache e o respectivo arquivo de cache no disco. Esta é uma ferramenta forense de uso geral que não limite apenas em trabalhar com itens de navegadores.

3.2 Uso geral

- *WinHex*

Descrição: Editor hexadecimal completo, que inclui cálculo de resumo de mensagem utilizando diversos algoritmos disponíveis, interpretador de dados em diversos formatos, busca por expressões regulares (similar ao grep do Linux), entre outras funções. Esta ferramenta apresenta diversas funções de extrema importância para a investigação forense, como: (Bueno, 2007)

- ✓ Interface especial para forense, incluindo criação de modelos de relatórios, criação da imagem do disco, análise do ADS (Alternate Data Streams) do NTFS, catalogação de arquivos, etc.;
- ✓ Possibilidade de aceder a memória principal com o sistema ligado, permitindo que os dados sejam copiados deste;
- ✓ *File carver* disponível para recuperar uma gama considerável de tipos de dados, sendo possível definir alguns critérios de pesquisa de cabeçalhos de arquivos se pretende procurar.

Desenvolvedor: X-Ways Software Technology AG/http://www.x-ways.net.

Licença: Proprietário.

- *Forensic Toolkit (FTK)*

Descrição: Ferramenta forense de uso geral com interface gráfica e com diversos recursos como busca avançada, capacidade de trabalhar com diversos formatos de arquivos, análise de arquivos ZIP, análise de e-mails e registo do Windows. Ainda, possui uma espécie de navegador embutido para visualizar conteúdo de cache de navegadores. Este pode classificar

e filtrar o conteúdo do cache para auxiliar a análise. Uma das suas desvantagem é o facto do processamento de arquivos de índice (index.dat) não permitir a geração de relatórios no formato de excel ou texto puro.

Desenvolvedor: AccessData/http://www.accessdata.com.

Licença: Proprietário.

- *EnCase*

Descrição: A ferramenta EnCase é uma das ferramentas mais completa no que se refere a perícia forense, porque para além de auxiliar na recuperação de arquivos deletados, padroniza laudos pericias, organiza Base de Dados com as evidências, encryption (fornece senhas do arquivo e o decrytion ("quebra" as senhas do arquivo) dos arquivos, analisa hardwares, analisa logs, analisa formatos e tipos de e-mails e ainda fornece uma opção de se manusear a evidência sem danificá-la, entre muitas outras funções. (Vargas, 2006)

Desenvolvedor: Guidance Software/http://www.guidancesoftware.

Licença: Proprietário.

- *CallerIP*

Descrição: O CallerIp, é uma ferramenta que auxilia o perito na indicação de entradas, saídas e invasões de IP na máquina em questão, informando qual o IP que está conectado ou tentando conectar-se apresentando no mapa de mundi a sua localização com endereço, telefone e responsável por aquele IP.(Vargas, 2006)

Desenvolvedor:/http://www.callerippro.com/index.html

Licença: Proprietário.

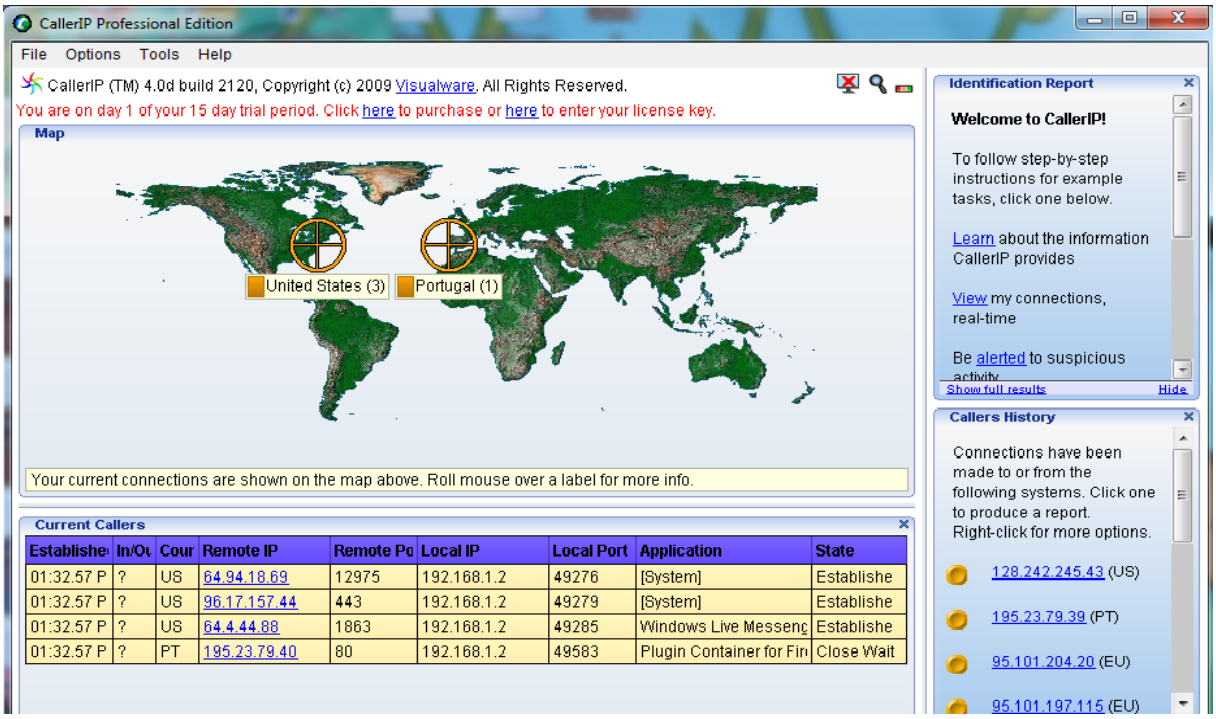

Figura 5 – Tela principal da ferramenta CallerIp

- *RecoverMyFile*

Descrição:Este é um programa que permite recuperar facilmente arquivosapagados acidentalmente, ou não do Windows. Para evitar que o arquivo apagado seja sobrescrito, essa ferramenta não requer instalação funcionando directamente em um disco flexível e funciona em qualquer versão do Windows que usa a tabela de partição de arquivos FAT e NTFS. Por outro lado, esta ferramenta suporta drives reconhecido pelo Windows com IDE, SCSI, USB, PCMCIA e outras interfaces.(Vargas, 2006)

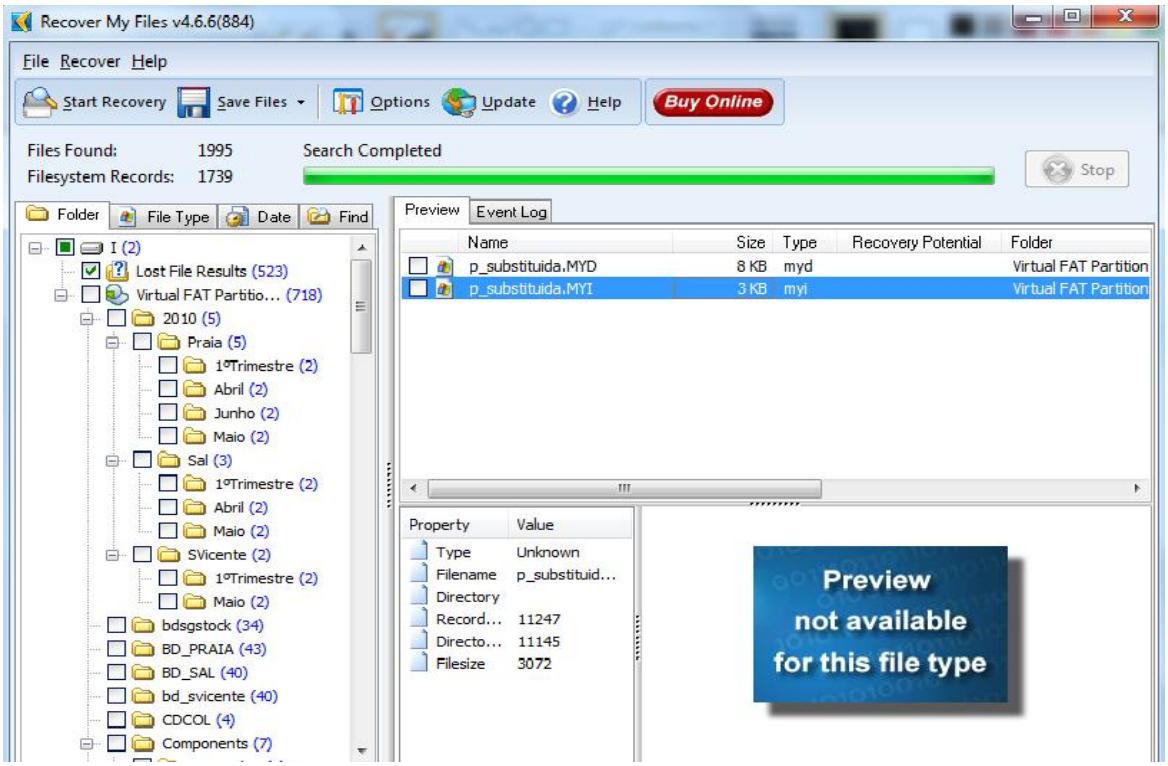

Figura 1 – Visualização de arquivos apagados na aplicação RecoverMyFiles

A figura 4, representa a tela principal da aplicação *RecoverMyFile* recuperando os dados apagados em uma determinada partição do disco que foram apagados propositadamente com o objectivo da sua visualização.

No lado direito da aplicação é apresentado os directórios que foram deletados. Do lado esquerdo, é apresentado o conteúdo dos directórios e abaixo é exibido as informações do ficheiro como por exemplo, o nome, tipo e tamanho do ficheiro.

Desenvolvedor: Getdata Pty, Ltd/http://www.recovermyfiles.com

- *FDTK-UbuntuBr*

Descrição: O FDTK-UbuntuBr – Forense Digital Toolkit, é uma distribuição Linux criada a partir da já consagrada distribuição Ubuntu, que reúne mais de 100 ferramentas capazes de atender a todas as etapas de uma investigação forense, oferecendo a possibilidade de ser utilizada como um liveCD e também ser instalado em um computador transformando-o em

uma estação forense. A referida distribuição está em constante evolução e é caracterizada não apenas pela quantidade de ferramentas, mas também por uma interface amigável, estruturada de acordo com as etapas do processo de perícia forense e ainda pela facto de ser distribuída no idioma português.(Lemes, 2007)

Figura 6 – Interface gráfica da FDTK-UbuntuBr

- *Low Orbit Ion Cannon (LOIC)*

O LOIC é software de código aberto escrito em C# desenvolvido pela Praetox Technoligies, e é categorizado como uma ferramenta de *Stress Network*, isto é, testar um aplicativo web exaustivamente para ver o quanto ele aguenta. Bastante usado para realização de ataques do tipo DoS e DDoS. (fonte: http://blog.corujadeti.com.br/loic-e-seus-pacotes-de-ions/)

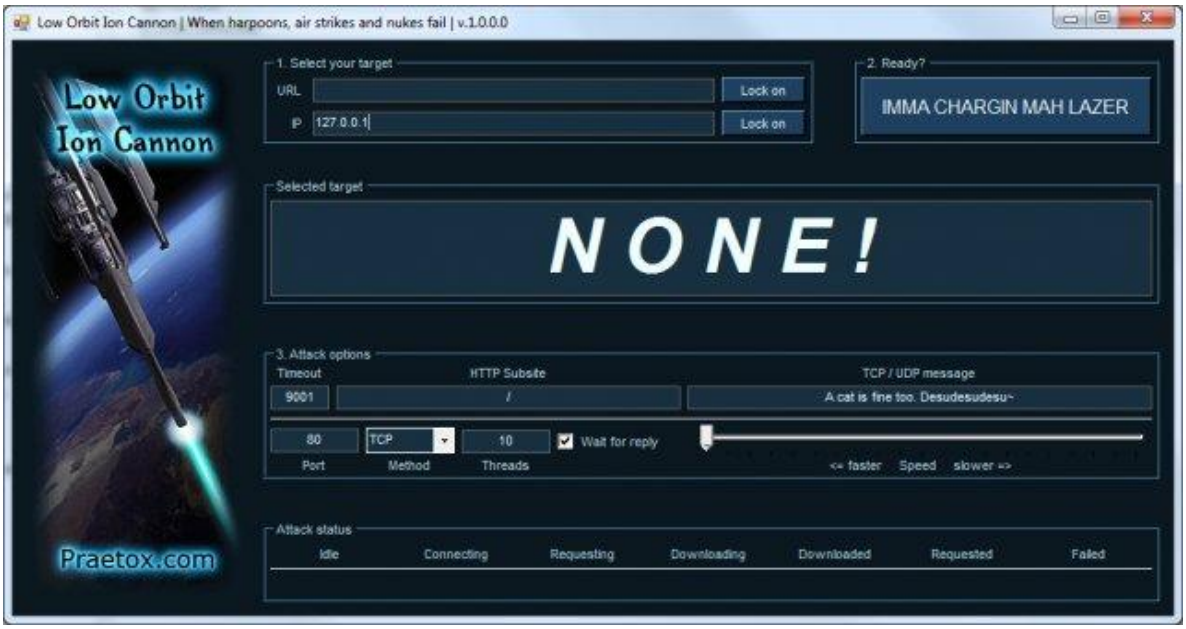

Figura 7 – Low Orbit Cannon (LOIC)

4 Enquadramento legal

O avanço tecnológico tem contribuído bastante para o aumento dos crimes electrónicos e, sem sombra de dúvida, pode-se afirmar, que os crimes informáticos aumentam em proporção da tecnologia. Portanto, os meios electrónicos, sobretudo a Internet, vem possibilitando cada dia a prática de crimes complexos e que vem por sua vez exigindo uma intervenção rápida e especializada.

Com o surgimento da informática e mais concretamente da internet, tornaram-se possível vários tipos de crimes electrónicos, o que indubitavelmente vem preocupando sobretudo as empresas, empurrando as agências legais a actuarem na investigação de casos que envolvem crimes desta natureza.

Normalmente, nos Países mais desenvolvidos onde existe uma legislação forte contra os crimes electrónicos, os criminosos da internet (hacker) tendem a fugir, pois já sabem que num país onde existe uma legislação forte serão facilmente sancionados no caso de cometerem

delitos. Portanto, esses criminosos ao fugirem tem tendência em refugiar-se para os países onde não existe uma legislação específica para esses crimes, ou se existe, então muito fraco.

Cabo Verde, apesar de não ter um **projecto-lei** específico contra vários desses crimes, tem mostrado preocupado com esta questão, pois, através de acordos e tratados internacionais já tem previsto em sua Lei alguns desses crimes (Artigo 11° e12° da Constituição de República).

4.1 A lei e a criminalidade informática

A TIC em Cabo Verde, é uma área nova e ainda na sua fase de crescimento. Como a criminalidade normalmente evolui em proporção da tecnologia, não podemos falar da tecnologia sem deixar de fazer referência a esta nova problemática[7] sobretudo em países em que está bem mais evoluída. Como por exemplo, Portugal já apresenta uma legislação própria contra crimes informáticos – a chamada Lei de Criminalidade Informática, com data em Agosto de 1991, estando dessa forma muito à frente do Brasil, que tem alguns projectos de lei em via do Congresso.

Em Cabo Verde, ainda não há uma cultura de informática jurídica e de direito da informática, para a necessidade de protecção de bens socialmente relevantes. Por outro lado, Cabo Verde ainda não tem uma legislação própria para os crimes informáticos. Desta forma, introduzir vírus em computadores, violação do direito do autor, copias de programas, etc, todos esses actos são, obviamente, criminosos, só que no nosso país ainda não há uma lei que define o que é crime dentro das novas tecnologias e desta forma, não os considera como crime (de acordo com o principio da legalidade, não há crime sem lei anterior que o defina).

Por outro lado, o facto de Cabo Verde estar a caminhar para uma sociedade de informação ou ainda, por se verificar uma crescente informatização nas suas várias áreas da actividade, isto vem criando novos problemas[8], que não existiam à poucos anos a traz com a utilização dos métodos manuais ou mecanográficos de tratamento da informação. Portanto, a evolução tecnológica representa um foco de atracção para os intrusos que estão sempre de olhos.

[7] Está-se a referir aos crimes informáticos
[8] Problemas de preocupação com a protecção das propriedades individuais ou empresarias.

Ainda, seguindo a mesma linha de raciocínio, Cabo Verde apesar de até a presente data não ter-seregistado estes problemas, poderá num futuro muito próximo vir a passar por estes tipos de problemas, por isso há que se ter uma visão previsível e não deixar até que as coisas aconteçam.

4.2 Legislação vigente

Segundo Dr. Henrique Borges, um advogado Cabo-verdiano experiente, citado por (Marques, 2006), o ambiente legal para o desenvolvimento das Tecnologias de Informação e Comunicação não se encontra ainda suficientemente regulamentado em Cabo Verde, estando mais configurado para as telecomunicações as quais constituem um dos eixos principais das TIC, não as abrangendo porém, em toda a sua dimensão.

De acordo com o nosso código penal, até o momento presente, só constituem crimes:

1) A inviolabilidade de correspondência e de telecomunicações, instituída pelo art. 43°da Constituição da República;
2) O acesso não autorizado aos meios informáticos (aos dados pessoais constantes do registos informático, as bases de dados de constituição das autoridades públicas e entidades privadas, aos arquivos, ficheiros, registos informático ou bases de dados para o conhecimento de dados pessoais relativo a terceiros (art. 44°da Constituição da República).

Muitos outros crimes não estão explícitos de forma clara na nossa Constituição, o que não significa que mediante a prática desses crimes estamos isentos (o crime pode ser enquadrado em uma lei internacional, desde que é de natureza internacional ou exista na ordem jurídica interna do país algum tratados e acordos sobre a matéria. - art. 12° da Constituição da República).

Como já mencionado anteriormente, o art. 11° da Constituição da República diz que o Estado de Cabo Verde rege-se, nas relações internacionais pelo Direito internacional e respeito pelos Direitos do homem.

CAPÍTULO 4: ESTUDO DE CASO – INVESTIGAÇÃO FORENSE NA MÁQUINA SUSPEITA

Neste capítulo, será apresentado um estudo de caso prático sobre a investigação em um sistema supostamente comprometido. O estudo terá duas fase: uma primeira que será implementadoe disponibilizadoum servidor web que permitirá a realização de ataques e consequentemente, uma segunda fase a investigação digital sobre o sistema atacado, aplicando as técnicas e metodologias forense citadas no capítulo anterior.

O servidor, foi preparado com todas as configurações possíveis e colocada a disposição de algumas pessoas (professores, colegas e amigos) para uma possível invasão. Tendo como objectivo tentando aproximar o máximo da realidade, não foi revelado nenhuma informação a respeito do Servidor como palavra-passe, nome de utilizador, entre outros. Foi fornecido apenas o endereço de nome: http://tstvulnerability.dyndns.ws.

1 Apresentação

Para o estudo de caso, foi instalado um PC com Windows 2000 e sem nenhuma actualização com o intuito de não dificultar o acesso. De seguida, foi instalado e configurado o serviço IIS de modo que permitisse posteriormente uma auditoria. Ainda, para poder-se auditar o acesso aos arquivos e pastas, foi ajustado algumas configurações a nível do Sistema Operativo.

Para visualizar melhor o estudo de caso, e garantir que o servidor está em funcionamento, foi criado e disponibilizado uma página web através do endereço acima referido para possíveis ataques.

1.1 Diagrama de rede

O esquema abaixo representa a arquitectura de rede usada.

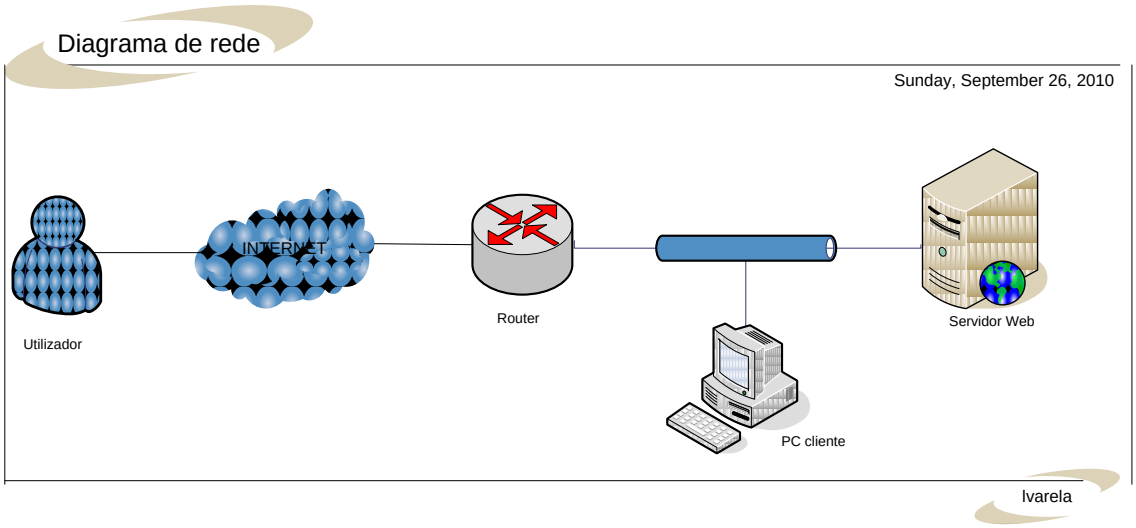

Figura 8 - Diagrama de rede:

Para que o estudo de caso se realiza-se com normalidade, foi preciso munir de um conjunto de recursos na qual se destaca:

- Um PC (servidor) com as seguintes características:
  - ✓ Sistema Operativo Windows 2000, SP3;
  - ✓ 39,3GB de Disco;
  - ✓ CPU 2.80GHz e 457,204 de RAM.
- Um Router de acesso a internet:
  - ✓ Modelo: Thomson ST546, 4 Interface Ethernet
- Um PC (cliente) para acesso remoto ao Servidor, com as seguintes características:
  - ✓ Sistema Operativo Windows 7 Professional;
  - ✓ 87,8GB de Disco;

- ✓ CPU 3.40GHz e 2.00GB de RAM.

1.2 Instalação e configuração do Servidor IIS 5.

O IIS 5.0 é o servidor web que vem juntamente com o Windows 2000 e para evitar ataques, não vem instalado por padrão. Por isso, foi necessário a sua instalação. Apesar de outras formas de instalação existente, no nosso caso foi optado o método "Adicionar e Remover Programas do Windows", como mostra a figura abaixo.

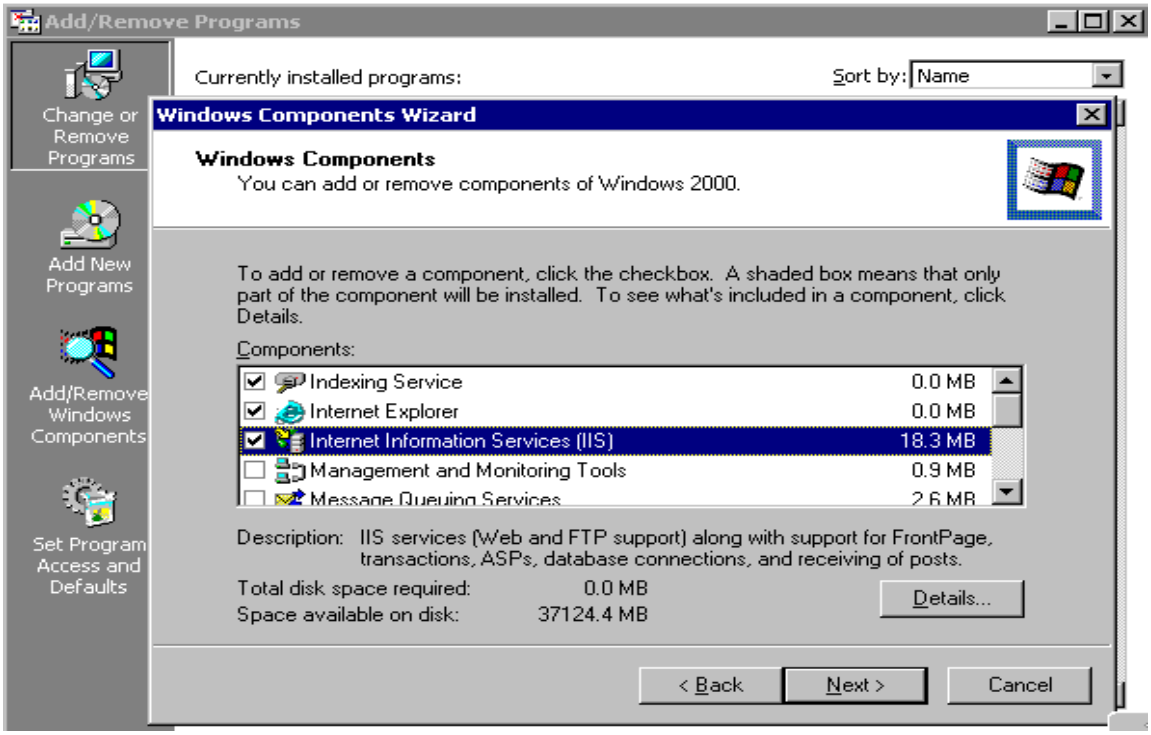

Figura 9 - Instalação do Servidor IIS 5.0

Após a instalação do IIS 5.0, foi efectuado um restart ao sistema e feito um teste para garantir que o IIS estivesse a funcionar. Para isso, foi digitado no browser (Internet Explorer) o endereço http://localhost e obteve-se o seguinte resultado:

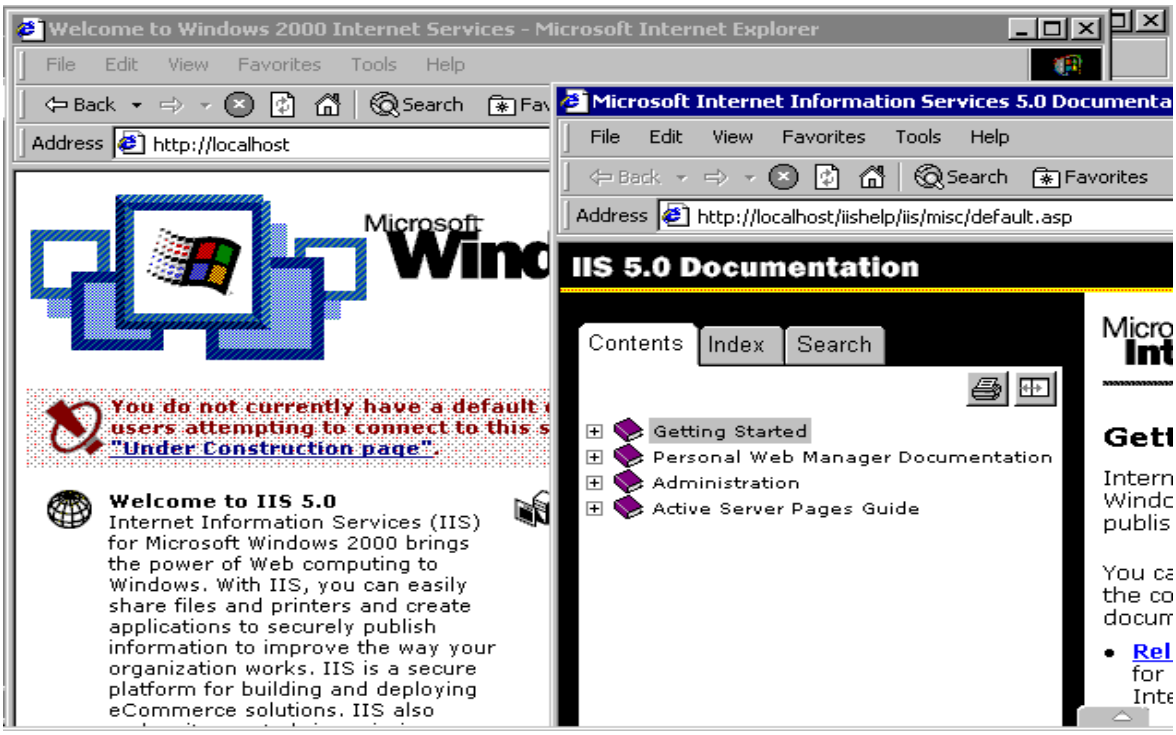

Figura 10 - Teste do Serviço IIS

Estando o servidor IIS a funcionar, passou-se pela configuração. Para isso, acedeu-se a janela de administração do Microsoft IIS 5 - localizado no directório**intsrv**(C:\Winnt\system32\intsrv\iis.exe) – Figura 11.

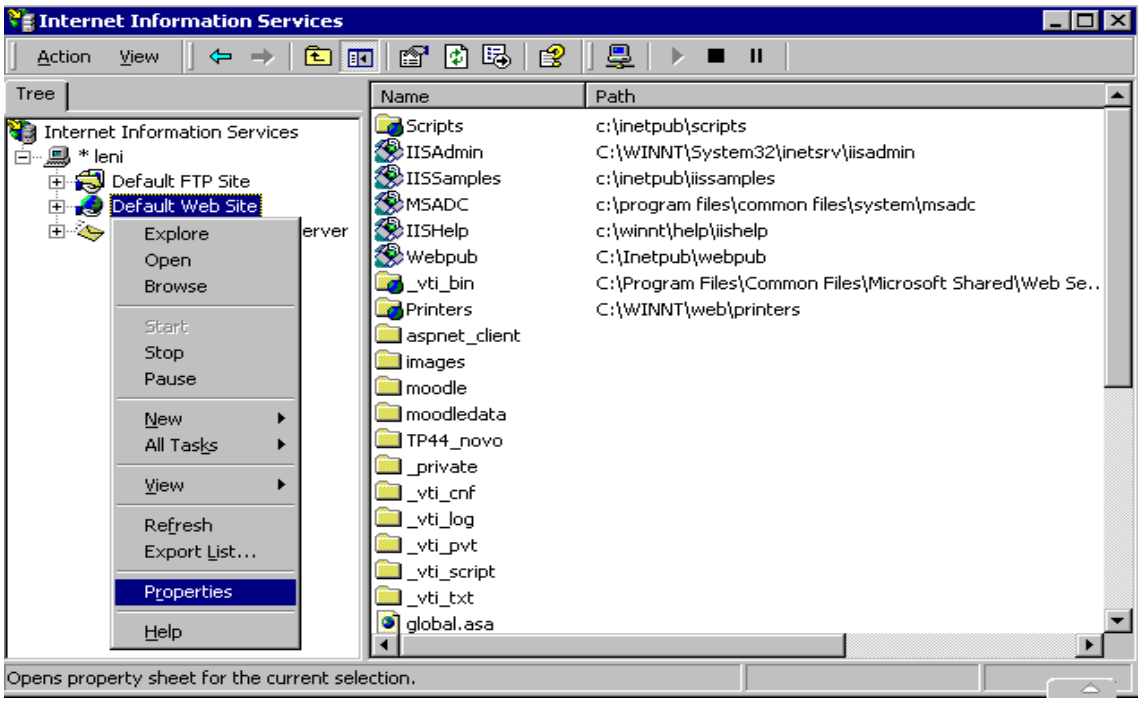

Figura 11 - GUI de configurações do Servidor Web

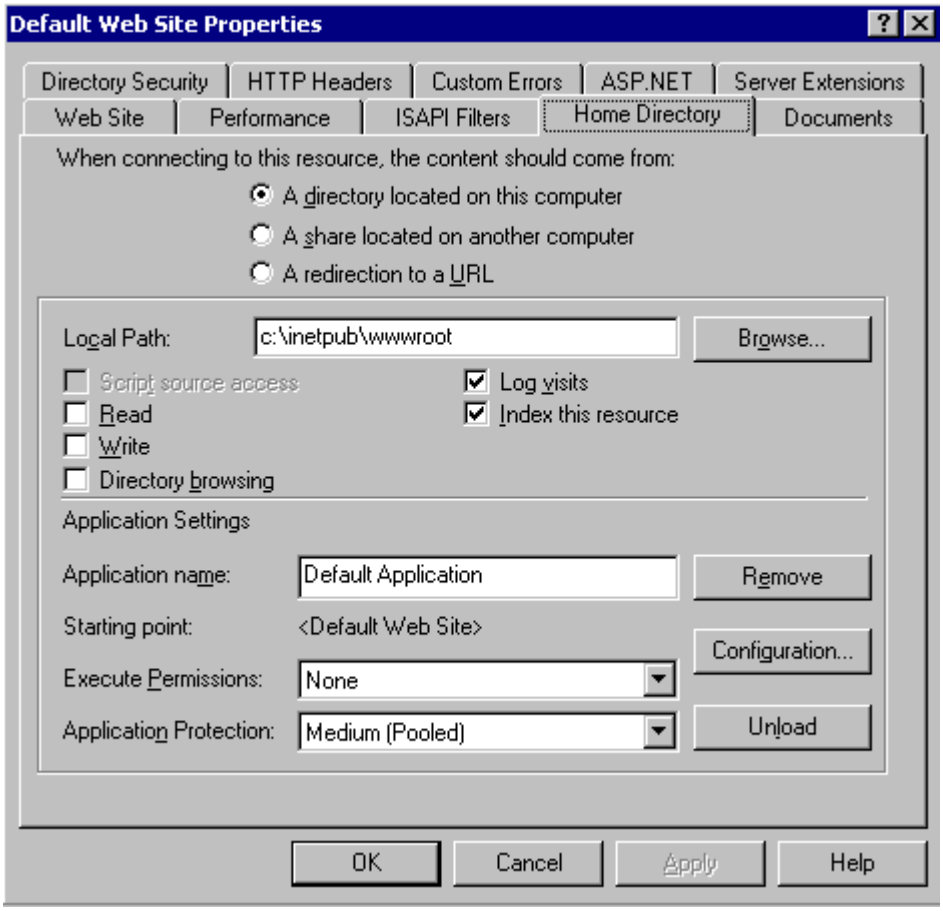

Figura 12 - Janela principal de configuração do Servidor IIS 5.

Esta é a janela principal de configuração do Servidor web. Nela fazemos todas as configurações como:

- **Home directory**: Indicamos a localização dos conteúdos acedidos pelos utilizadores e as suas respectivas permissões. Apesar disso, pode-se redireccionar os pedidos para uma directoria específica. Deve-se ter cuidado na questão de permissões, pois se não for dado as devidas permissões os utilizadores não conseguirão aceder os conteúdos.
- **Documents**: Representa a ordem de procura do documento padrão do site. Para que os pedidos sejam redireccionados para uma página específica.
- **Directory security**: No momento de publicação do site, é preciso tomar algumas medidas de segurança. Por exemplo, qual o tipo de autenticação será feita por este site, se o utilizador anónimo será habilitado, se tem alguma faixa de IP que precisa ser

bloqueada, se é necessário o uso de certificado digital por parte do utilizador para aceder ao site.

- **Custom error**: Para configuração das páginas de erros para os utilizadores e log de erros do site (acessível via arquivo texto).
- **Web Site**: Permite configurar os arquivos de logs do servidor de aplicação do Windows e a definição da porta TCP. Por padrão, vem a porta 80 e W3C como arquivo de log.

1.3 Configurações a nível do Sistema Operativo

O Windows dispõe de vários recursos e ferramentas integradas para incrementar sua operacionalidade. Vários desses recursos são acessíveis e configuráveis directamente no Painel de Control. Outros, no entanto, permanecem escondidos. Isso pode dificultar os utilizadores. Mas, em compensação, existe outro menu dedicado exclusivamente para edição desses recursos, conhecido como snap-in. Neste caso específico foi preciso usar o snap-in da Política de Grupo para activar a configuração da auditoria.Após ter feito isto, foi visualizado o log de segurança em "Visualizador de Eventos" para ver as tentativas aceitadas e não aceitadas de acesso as pastas e arquivos auditados.

Para activar a auditoria de segurança no Windows 2000, acedemos ao Painel de Control e escolhemos "Política de Segurança Local" como mostra a figura abaixo.

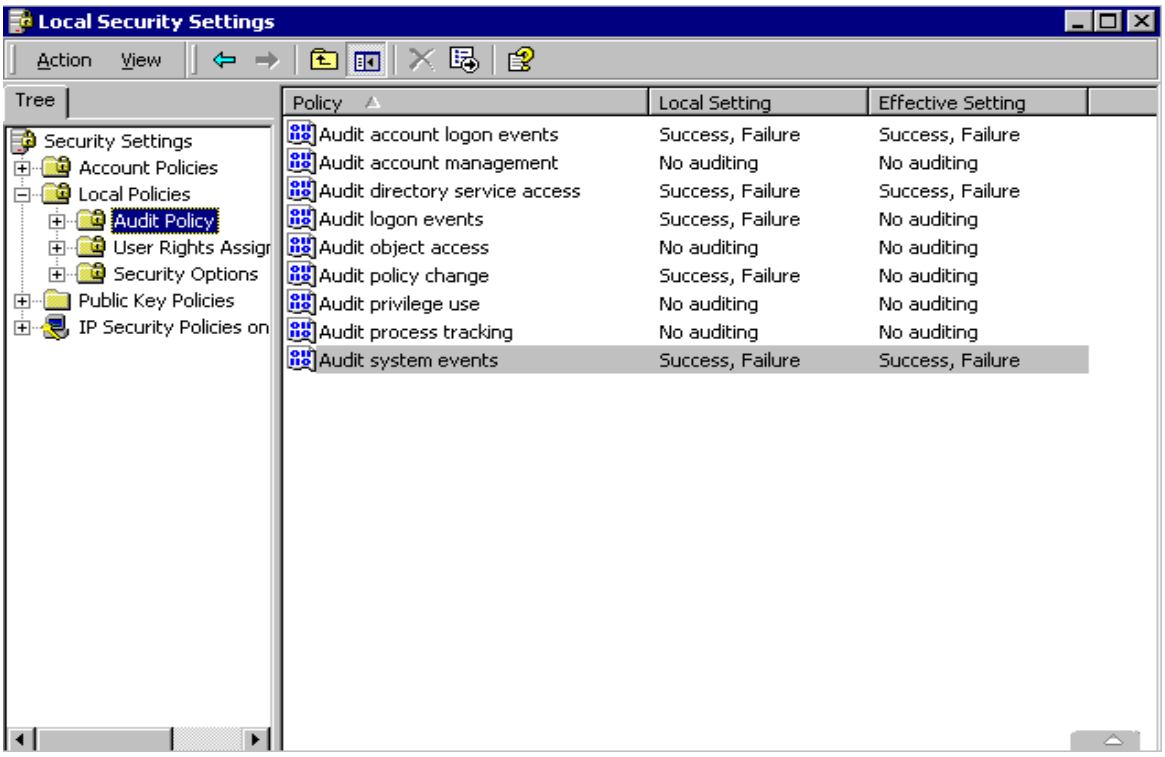

Figura 13 - GUI de configuração da Auditoria de Segurança

1.4 Configurações a nível do Router

O router usado é o modem ADSL disponibilizado pela CVMultimédia. Embora com algumas restrições de segurança, oferece os recursos mínimos para configuração. Uma das configurações é o Dynamic DNS.

O Dynamic DNS, é uma funcionalidade do router que serve para ir actualizando o nosso IP no servidor do DynDNS, cada vez que este for alterado, isto porque o IP usado para cessar a internet é dinâmico.

Antes de poder usar esta funcionalidade, foi necessário criar uma conta no DynDNS através do site www.dyndns.com. Uma vez criado a conta, o próximo passo foi fazer o registo de nome do site, ou seja, adicionar um host a nossa conta de DynDNS.

Para terminar, acedeu-se a ferramenta “Dynamic DNS” do router e introduziu-se os dados de configuração solicitados abaixo (figura 12).

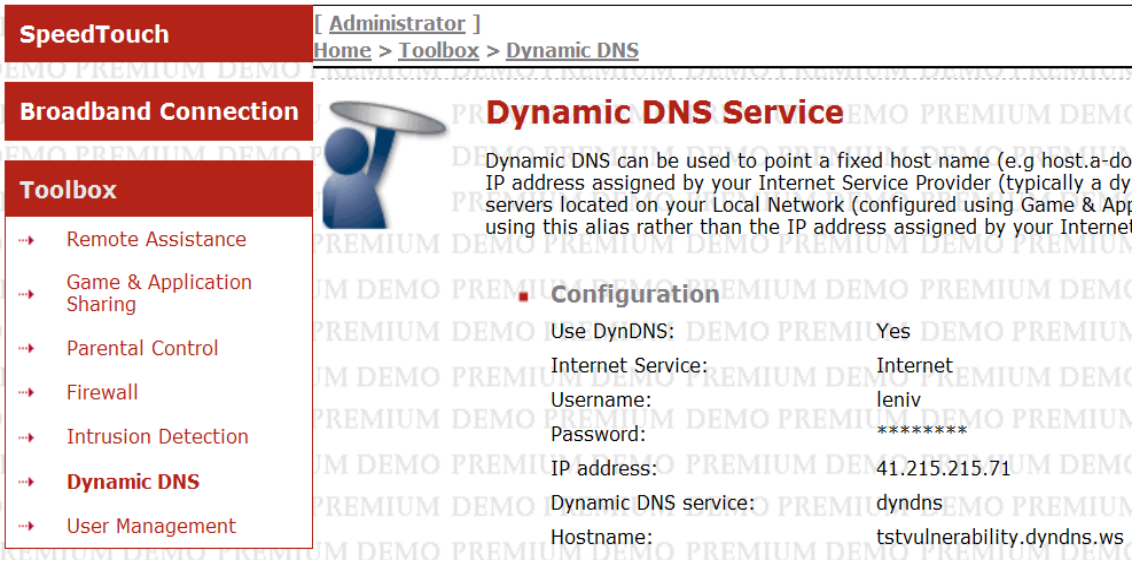

Figura 14 - Configuração do Dynamic DNS

O router, através do Dynamic DNS, executará as seguintes tarefas:

- Mantém comunicação constante com DynDNS.com, actualizando o seu hostname para resolver o endereço IP remoto;
- E determina automaticamente qual interface de rede a usar, detecta automaticamente proxies.

1.4.1 Realização de testes

Após ter terminado todo o processo de configuração, chega-se a parte de maior ansiedade: ver o servidor a funcionar como desejado.

Primeiramente, foi efectuado um PING para o endereço de nome, com o intuito de saber se é feito a resolução de nome. O endereço foi resolvido com sucesso (Figura 15).

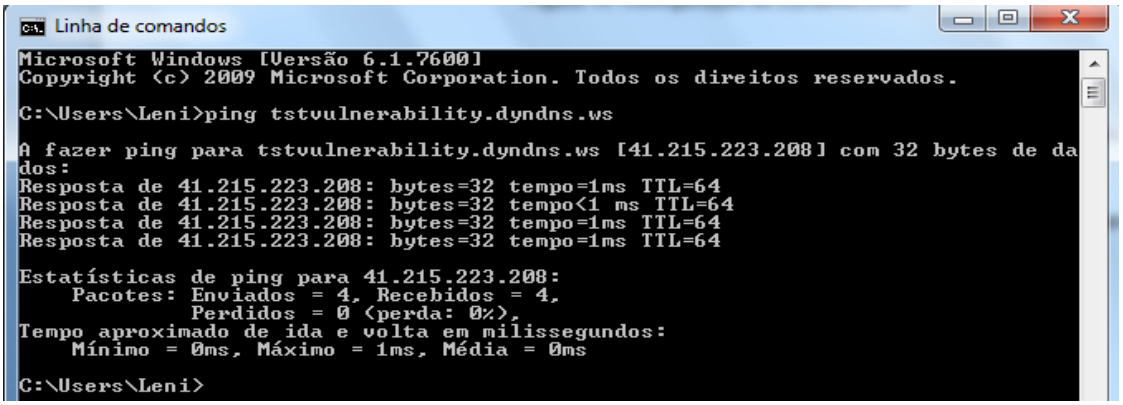

Figura 15 - Teste de resolução de nome

Ainda, foi criado uma página web e hospedado no servidor. A partir de um máquina com acesso a internet (fora desta rede),foi acedido a partir do endereço http://tstvulnerability.dyndns.ws/ e obteve-se como resultado (figura 16):

Figura 16 - Teste servidor – página web

1.5 Testes de intrusão

Para a realização de simulações de ataques foram utilizadas algumas ferramentas hacking no que se destaca:

- **Advanced Port Scanner:** Ferramenta usada para varredura das portas abertas que permitem acesso a máquina. Para testar as vulnerabilidades do servidor, foi necessário correr a aplicação "Advanced Port Scanner" que por conseguinte retornou as portas abertas e fechadas no servidor.

Figura 17 – Varredura de portas

Como se pode constatar, após uma varredura de rede, verificou-se que o referido servidor, alvo de ataque, encontra-se com 3 portas abertas: Porta 21 – FTP, 23 – Telnet e 80 – http, o que pode facilitar entradas individas.

- **Brutus AET2:** Ferramenta usada durante o teste de intrusão para ataque de passwords.

Como se pode constatar, o endereço IP da máquina a ser invadida utilizado foi **41.215.214.81**, serviço http com autenticação básica **http (Basic-Auth)**. Na secção "Authentication Option" foi indicado a forma de pesquisa e depois o arquivo de nomes de utilizadores determinado no campo "User File" para verificação de vários

logins. O modo de tentativas de login utilizado foi **Brute Force**, por ser mais eficiente, permitindo diversas combinações com os caracteres específicados.

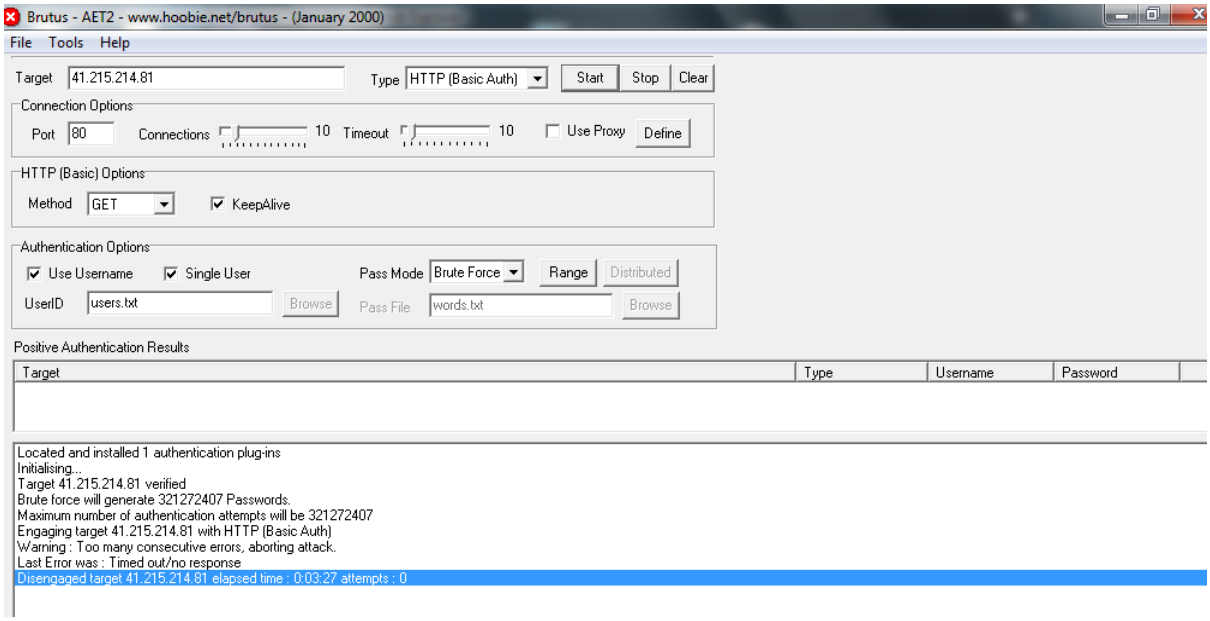

Figura 18 – Ataque de Brute Force

- **Low Orbit Ion Connon (LOIC)**

  Para ataques do tipo DoS, foi usado a ferramenta LOIC. Para indicar que o ataque é do tipo DoS, foi seleccionado a opção Manual Mode, colocar endereço ou IP do site alvo em URL/IP, na opção Method foi escolhido o protocolo e de seguida a porta que o LOIC irá tentar conctar. Em cima temos o botão IMMA CHARGIN MAH LAZER, que serve para disparar o ataque. Por fim, temos em baixo o Attack status que apresenta as estatísticas do ataque.

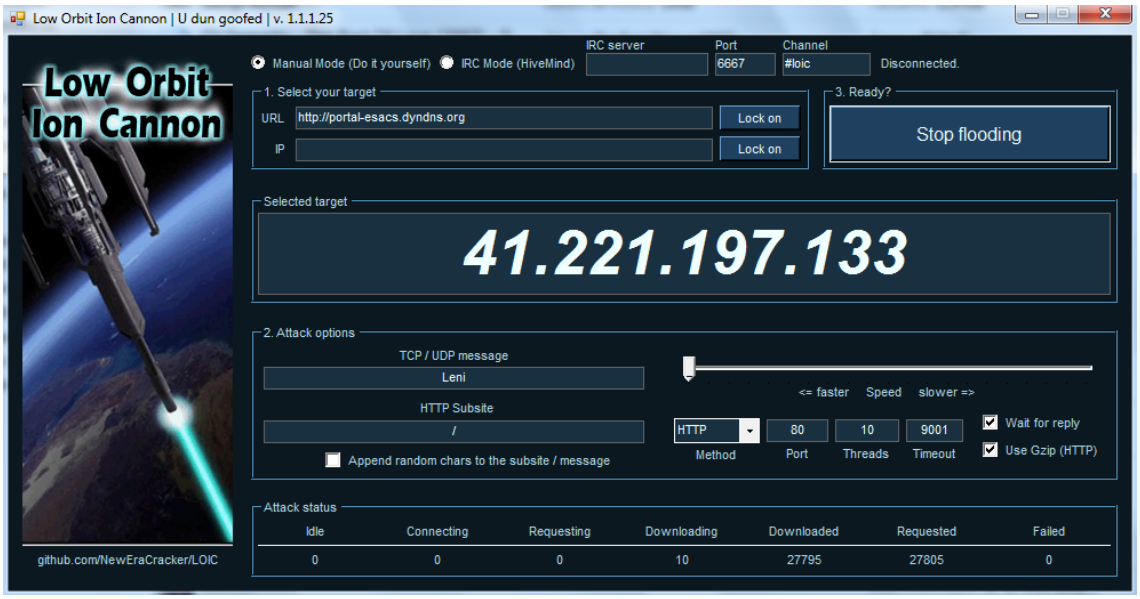

Figura 19 – Ataque do tipo DoS- iniciado

1.6 Considerações Finais

O estudo de caso teve como objectivo, a consolidação dos conhecimentos teóricos adquiridos ao longo do trabalho.

Pode-se concluir e com convicção, que os objectivos preconizados foram todos atingidos, o que se pode explicar pelas acções levadas a cabo durante o estudo de caso.Houve alguns constrangimentos relativamente ao estudo de caso, mas estes foram ultrapassados.

2 Investigação

Após ter sido apresentado como são os formatos dos arquivos de logs do servidor Web IIS da Microsoft e suas características, inicia-se agora um estudo de caso em que um Servidor Web foi invadido, deixando rastos bem visíveis. Será demonstrado como o hacker entrou no sistema, de onde veio o ataque e qual foi a alteração ocorrida no sistema.

A investigação será feita sobre uma máquina com Sistema Operativo Windows 2000 Profissional, Serviço IIS 5.0 e com configuração de arquivo de log no modo W3C.

Os campos importantes que serão utilizados para investigar incidentes suspeitos incluem o registro data/hora, endereço IP de origem, código do status do HTTP e recurso requisitado

2.1 Apresentação

Após ter disponibilizado o servidor na internet por 5 (cinco) dias para invasão, foi feita uma análise de cada pasta na qual o IIS guarda as suas configurações e constatou-se que houve alguns eventos ocorridos que poderão ou não corresponderem acções maliciosas. Por exemplo, o ficheiro de log do servidor alvo demostra que houve alguns ataques e várias tentativas de ataques.

2.1.1 Registos de Ocorrências

Durante os cinco dias de testes, houve vários acessos a página, com alguns incidentes registados como será demostrado abaixo:

Ocorrência #1: Registos de acesso a página

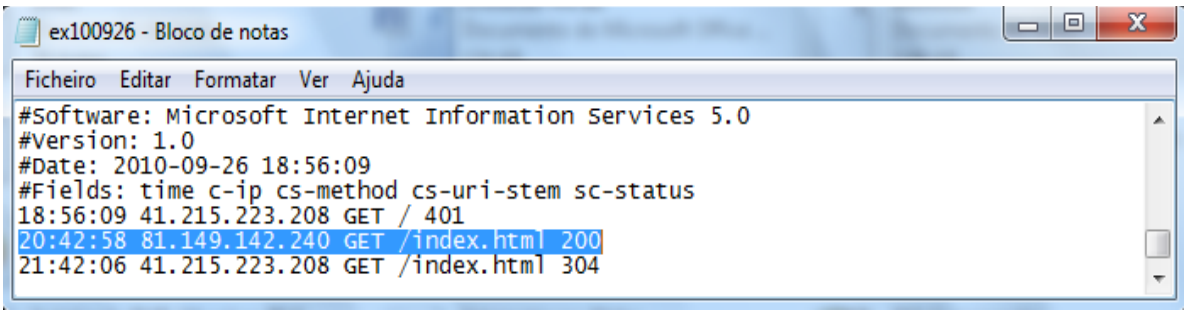

Figura 20 - Arquivo de log W3C

Como podemos observar, no dia 26 de Setembro de 2010 às 18:56, um utilizador com versão 1.0 de aplicação HTTP e com endereço IP:81.149.142.240 emitiu um comando GET do HTTP para um arquivo index.html. A solicitação foi interpretada sem erro.

Ocorrência #2: Espelhamento do site

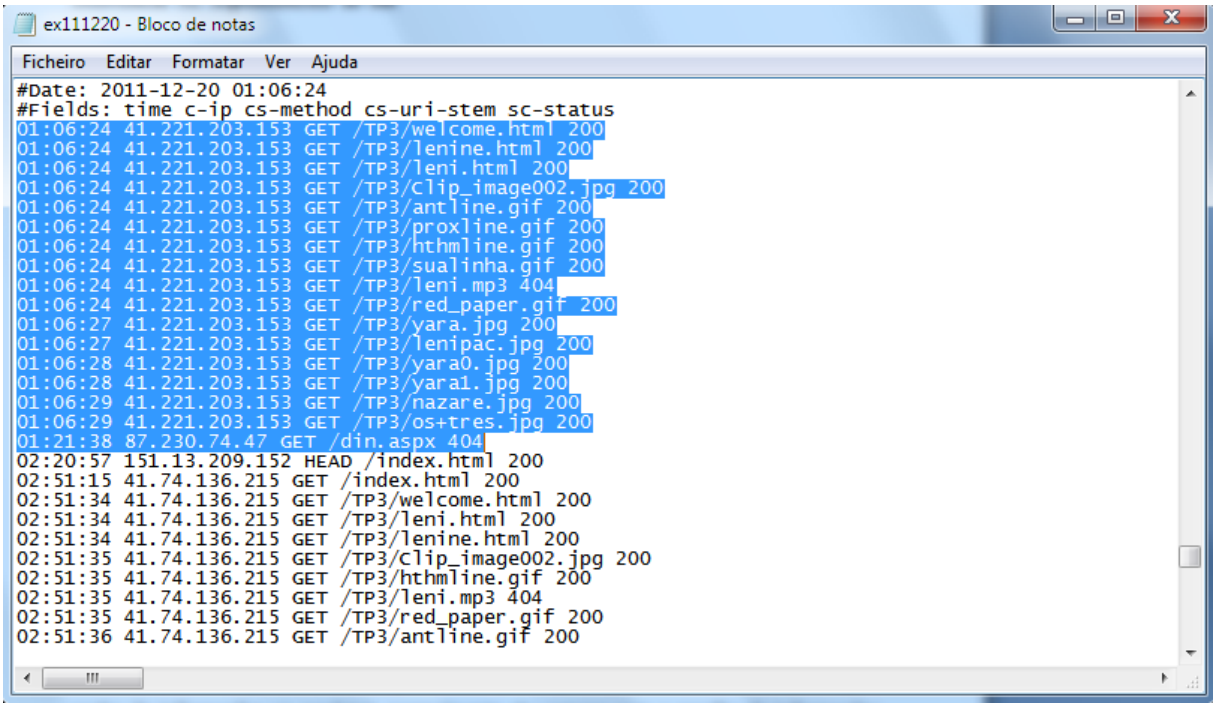

Figura 21 – Espelhamento de site

Se um invasor tem por finalidade específica lançar ataques contra site de uma empresa (para roubo de informações ou produto), normalmente ele começa com a recolha de informações. Primeiro irá determinar quais as informações sobre o software e funcionalidade do servidor Web estão disponíveis, podendo utilizar um "site espelhado" para estudo. Embora não seja ilegal e não indique um ataque por si só, quando esse tipo de recolha de informações é combinada com outras atividades, o investigador deve desconfiar. Para examinar a total funcionalidade do site, o invasor espelha o site, copiando cada página para examiná-las em detalhes off-line. Para o IIS, essa atividade deve aparecer como muitos pedidos do mesmo IP de origem durante um curto período de tempo.

O ficheiro de log apresentado acima, demostra claramente que antes do ataque, houve um espalhamento do site. Mostra que o invasor copiou as páginas para uma possivel análise.

Ocorrência #3: Varredura de vulnerabilidades

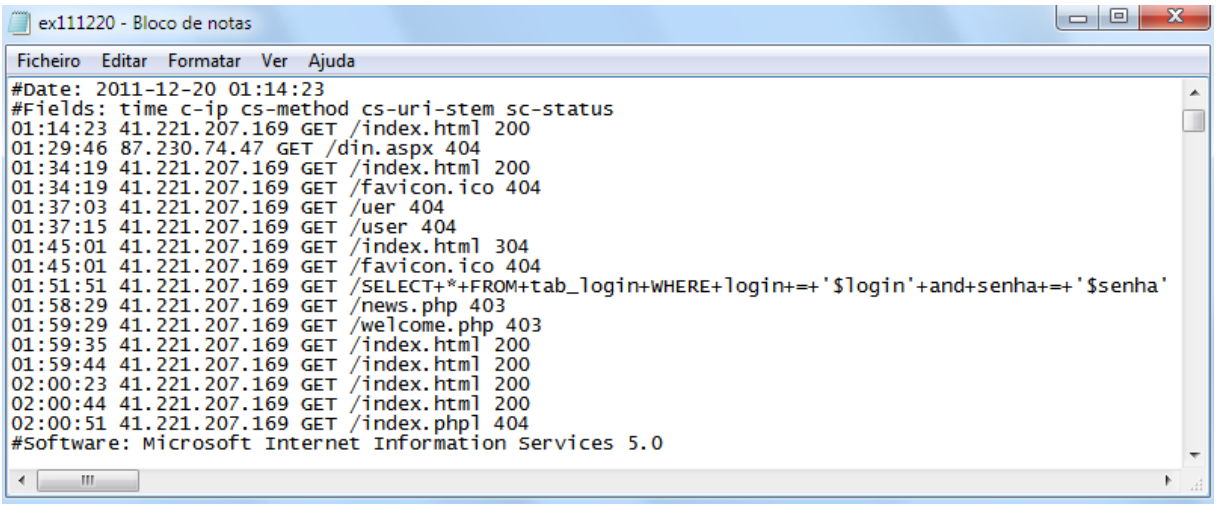

Figura 22 - Varredura vulnerabilidades

Depois de reunir informações sobre o servidor Web e criar o espelhamento do site, o invasor começou a "varredura da vulnerabilidade no servidor. A Figura 17, mostra que o servidor web em causa recebeu inúmeras sondagens, varreduras (scans) e consultas diariamente.

Como se pode ver, os detalhes-chaves procurados no referido ficheiro de logs, são pedidos repetidos de recursos que resultaram em códigos de erro sendo retornado ao cliente. Qualquer varredura de vulnerabilidade procurando por páginas vulneráveis inevitalvelmente resultará em muitos códigos de erro do tipo 404 ("arquivo não encontrado – file not found"). Além disso, o endereço IP de origem mantém estável em um curto intervalo de tempo, o que se verifica no log acima.

Ocorrência #4: Ataques DoS – Negação de serviço

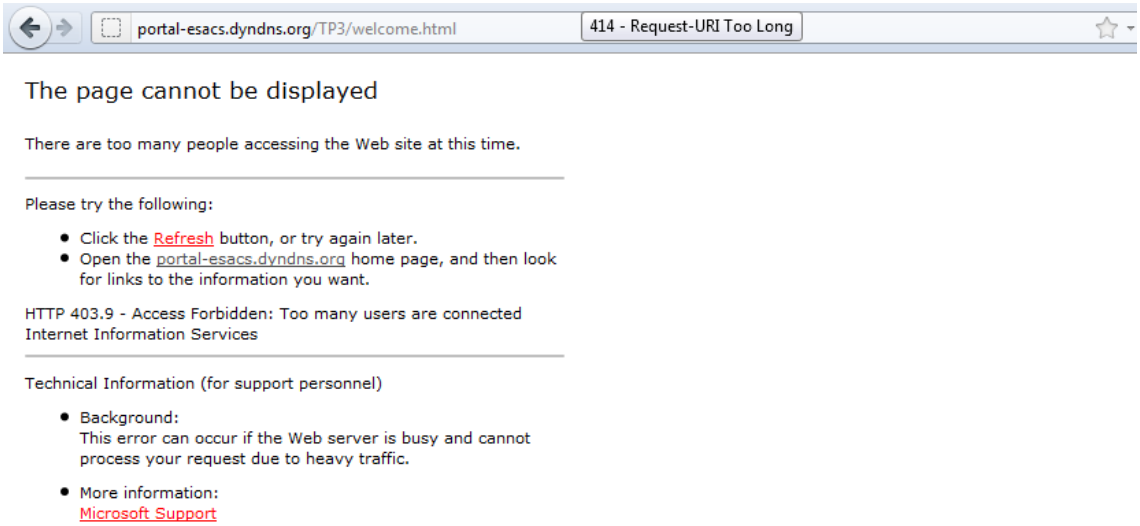

Figura 23 – Ataque de Negação Serviço

Como se pode verificar, após a realização do ataque do tipo Negação de Serviço, utilizando a ferramenta LOIC, o servidor ficou indisponível. Tentou-se aceder por várias vezes a página, mas sem sucesso.

Ocorrência #5: Ataques por injecção SQL

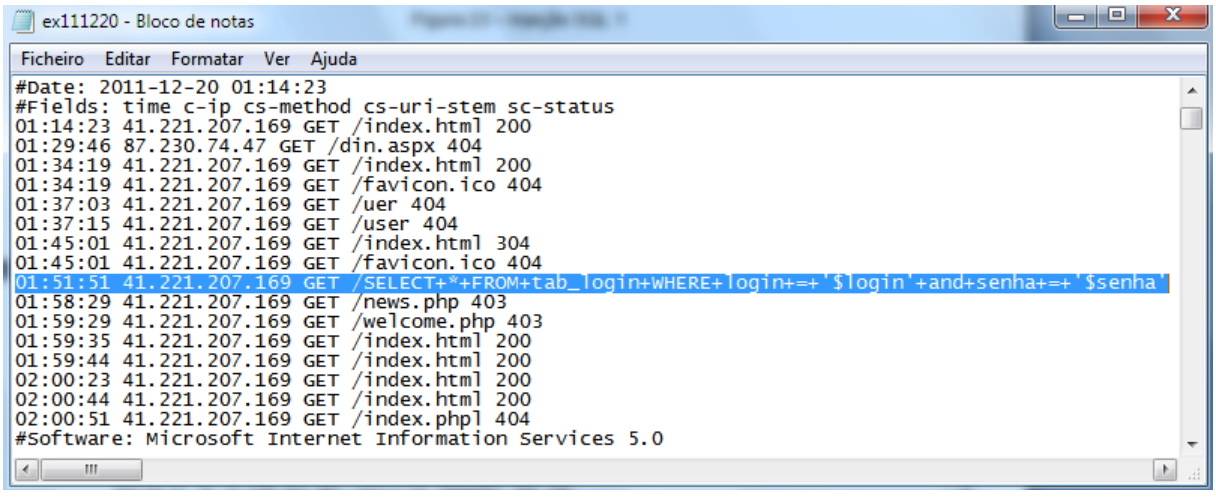

Figura 24 – Injeção SQL 1

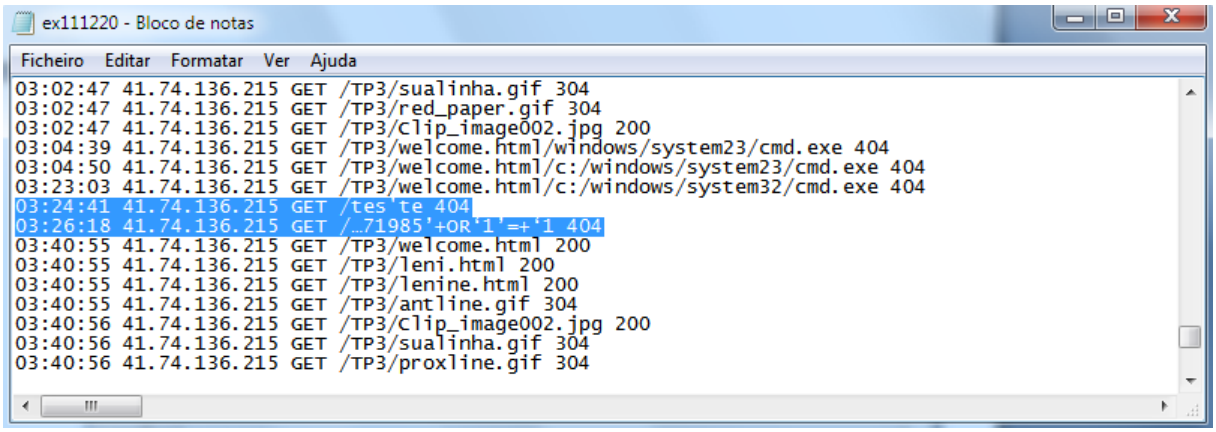

Figura 25 – Injecção SQL 2

De acordo com os logs acima, houve tentativas de ataques por via de injecções SQL. Tudo indica que o invasor digitou a palavra "**tes'te"** no campo nome para autenticação, mas sem sucesso. O código de erro 404 indica ataques sem sucesso. O ataque não se concretizou por duas razões: não existência de uma base de dados ou porque a base de dados está protegida contra esse tipo de ataque.

Ocorrência #6: Eventos de windows

Foi analisado os logs de eventos do Windows a procura de algum rasto de criação de contas de utilizadores ilegais com privilégios de administrador, mas não foi encontrado nenhum vestígio.

Também, foi analisada cada pasta na qual o IIS guarda as sua configurações,com o intuito de descobrir se houve alterações ou modificações numa desta pastas, já que esta tem sido uma prática muito comum usada pelos atacantes. A figura abaixo mostra que não houve criação nem alteração nos arquivos.

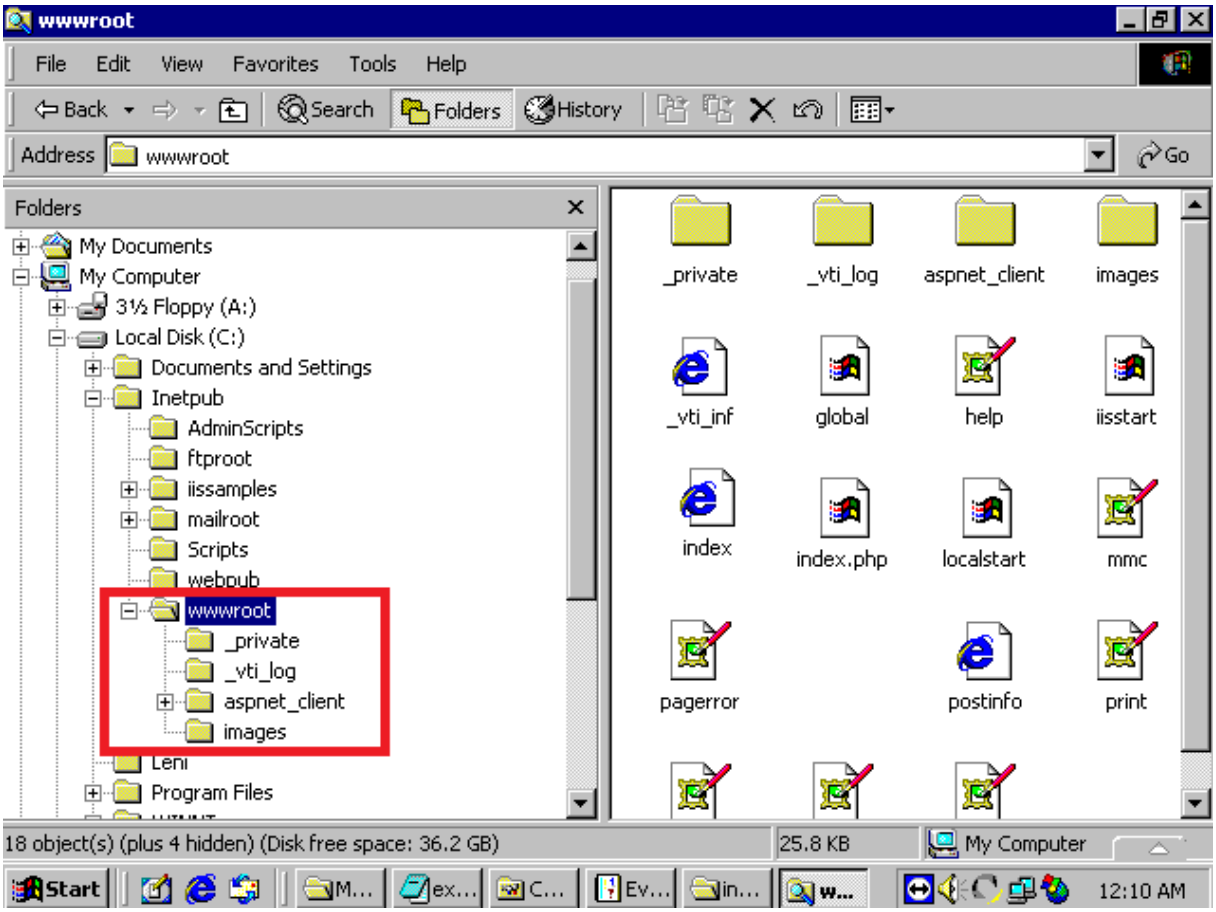

Figura 26 - Verificação de arquivos alterados

Ocorrência #7: Registo do router

De acordo com log do IDS (Router), o que se pode constatar, é que foram lançadosao servidor dois tipos de ataques: TCP_NULL_PORT e UDP_PORT_SCAN (Figura 19).

A **UDP_PORT_SCAN**, é um ataque de varredura de porta. Esta, é um dos ataques mais conhecidos quando se deseja descobrir serviços vulneráveis em um servidor. Esta é a primeira coisa que o invasor faz ao tentar atacar um servidor.

A **TCP_NULL_PORT**, é um ataque em que não se tem resposta para portas abertas. Nesta varredura, é enviado um flag nula (activa), se não receber uma resposta a porta está aberta, mas se receber um RST a porta está fechada.

Intrusion Name	Count
fragment_sweep	0
zero-length_fragment_size	0
tcp_null_port	1
fragment_size_overrun	0
fragment_overlap	0
fragment_out-of-order	0
ip_protocol_scan	0
tcp_port_scan	0
tcp_syn_scan	0
stealth_tcp_null_scan	0
stealth_tcp_fin_scan	0
stealth_tcp_xmas_scan	0
stealth_tcp_full_xmas_scan	0
stealth_tcp_vecna_scan	0
stealth_tcp_syn-fin_scan	0
udp_port_scan	4
ping_sweep_scan	0

Figura 27 - Log IDS

2.2 Considerações Finais

Diversos arquivos de logs foram auditados para confirmar ou não se um incidente ocorreu. No entanto, não foi encontrado nenhum indícios legais que comprovam a existência de crimes. Isso leva a concluir que durante este período de tempo não houve ataques, ou então se houve, provavelmente foi praticado por um intruso com elevado nível de conhecimento e experiência ao ponto de limpar os vestígios.

CAPÍTULO 5: CONCLUSÃO

O avanço tecnológico tem contribuído bastante para o aumento dos crimes electrónicos e, sem sombra de dúvida, pode-se afirmar, que os crimes informáticos aumentam em proporção da tecnologia. Portanto, os meios electrónicos, sobretudo a Internet, vem possibilitando cada dia a prática de crimes complexos e que vem por sua vez exigindo uma intervenção rápida e especializada.

No âmbito deste trabalho de investigação e face aos objectivos preconizados, foi abordada as tácnicas de ingestigação forense em servidor IIS do windows. Para uma maior valência e consolidação dos conchecimentos adquiridos durante o estudo, achou-se necessário a aplicação dum estudo de caso. No final desse estudo chegou-se as conclusões a seguir registadas:

Para além de não existir uma legislação específica que regule os crimes de natureza informática, há escassez de profissionais na área de direito da informática e de investigação forense computacional. Por outro lado, verificou-se que em Cabo Verde, ainda não há uma cultura de informática jurídica e de deireito de informática devido a violação constantes sobretudo de direito do autor e distruibuição e comercialização de softwares proprietários.

A terefa de investigação forense computacional não é fácil, pois exige um alto nível de conhecimento por parte do investigador. Apesar de algumas deficuldades encontradas durante

a realização deste estudo, por ser esta uma área nova, com poucos estudos ainda no mercado, ganhou-se muito em termos de conhecimentos.

Relativamente ao estudo de caso, parte prática do trabalho, também ganhou-se muito em termos de conhecimentos, pois foi colocado em prática os conhecimentos teóricos abordados no trabalho. Todavia, não foi fácil a análise forense devido a experiência do perito. Por outro lado, a máquina foi disponibilizado para ataques por um tempo muto curto devido as limitações do tempo o que dificultou na recolha de dados. Sendo assim, não limitou-se apenas aos recursos da IIS para investigação, mas também os recursos do Sistema Operativo e do router.

Um outro detalhe importante que não pode-se deixar passar despercebido, é a questão da legislação cabo-verdiana no domínio da informática. Houve dificuldades no enquadramento legal das evidências, pois ainda em Cabo Verde, não existe uma legislação específica sobre a criminalidade informática. Entretanto procurou-se ponderar dentro das limitações da nossa legislação.

É importante aínda frisar que dos diálogos estabelecidos com alguns administradores de redes, deu para concluir que a tomada de consciência e a experiência destes, no domínio da forense são ainda limitadas, pelo que pode ter havido muitas intrusões que não foram detectados.

Recomendações

Recomenda-se a todas as empresas ou instituições que lidam com informações de alto nível de confidencialidades e as instituições legais ou de combates aos crimes de natureza informática:

- **No domínio da legislação**:

  1. A Criação de uma legislação específica que tipifica as condutas criminosas na internet, pois a inexistência desta legislação constitui verdadeira garantia de impunidade aos criminosos virtuais;
  2. Investir na formação e capacitação dos nossos quadros de modo a adquirirem competências que os permitam identificar as ocorrências de crimes. Normalmente os intrusos não têm medo de invadir sistemas, pois já sabem que há carência de profissionais especialistas em forense computacional.

- **No domínio de segurança**:

  1. Manter actualizado o Sistema Operativo;
  2. Utilização de senhas criptografadas
  3. Prevenção de ataques via LOIC. Para previnir-se especialmente contra esse tipo de ataques (Negação de Serviço), recomenda-se limitar o número de requisições por segundos para cada endereço IP. Isso pode ser feito via lighttpd juntamente com um firewall, por exemplo através do NetFilter (ipTables).
  4. Utilização de um bom sistema de Identificação de Intrusão (IDS), como o snort, por exemplo.

- **No domínio da investigação Forense**:

  1. Para os professionais de área, durante a investigação forense, usar metodologias bem definidas que permite garantir qualidade a fim de assegurar a confiabilidade e a precisão das evidências;
  2. Documentar todos as provas recolhidas;

Bibliografia

Bueno, M. (2007). *Forense Computacional: Técnicas e Ferramentas*. Disponível em: http://www.las.ic.unicamp.br/paulo/teses/. Acessado em: 14/08/2010.

Baker et all (2010). 2010 DATA BREACH INVESTIGATIONS REPORT: *A study conducted by the Verizon RISK Team in corporation with the United States Secret Service*. Disponível em: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf. Acessado em: 20/09/2010.

Borges, P., & Coutinho, R.(2007). ANÁLISA DE SISTEMAS DE DETECÇÃO DE INTRUSOS EM REDE DE COMPUTADORES. Disponível em: http://www.snort.org.br/arquivos/Monografia-pedro.pdf. Consultado em 17/08/08. Acessado em: 03/05/2010.

Costa, A. (2005). *IPCop Firewall - Uma ótima opção de proteção para sua rede ADSL*. Disponível em:http://www.vivaolinux.com.br/artigo/IPCop_Firewall_-Uma_otima_opcao_de_protecao_para_sua_rede_ADSL/. Acessado em: 10/05/2010.

Cezar, G.(2006).*Computação Corporativa*: Especial para o Computerworld. Disponível em:http://idgnow.uol.com.br/computacao_corporativa/2006/06/21/idgnoticia.2006-06-21.5687122771/. Acessado em: 02/08/08

Castro Jr et all (S/D). Forense Computacional em Memória Principal. Disponível em:http://www.mp.go.gov.br/portalweb/hp/1/docs/foren-comp-ram.pdf. Acessado em: 01/05/2010.

Freitas, A.(2006). "Perícia Forense Aplicada a Informática", 1ª edição, Editora BRASPORT Livros e Multimídia Ltda, SP, Brasil.

Freitas, A.(2003). "Perícia Forense Aplicada a Informática". Disponível em: http://www.linuxsecurity.com.br/info/general/andrey-freitas.pdf. Acessado em: 09/08/2010.

ID TECH. (2006).Value Added Solution. Disponível em:http://www.idtech.com.br/sol_atm.asp. Acessado em: 02/08/2010.

LIM-APO, D.(2004). Aplicação de Técnicas de Forense Computacional Respostas a Incidentes na Internet. Disponível em:http://www.istf.com.br/vb/pericia-forense/7809-aplicacao-de-tecnicas-forense.html. Acessado em 20-05-2010. Acessado em: 12/03/2010.

Lemes, L.(2007). FDTK-UbuntuBr – Forense Digital Toolkit. Disponivel em:Site:http://www.dicas-l.com.br/dicas-l/20071207.php. Acessado em:28/08/2010.

Penedo, D.(2007). *DAR II:Desenvolvimentos avançados de rede II – Segurança*. REDE DE DETECÇÃO DE INTRUSÃO. Disponível em:http://www.fccn.pt/eci/doc_eci10/IDS-DARII-1.1.pdf. Acessado em:29/07/2010.

Reis, M., A. (2003). Forense computacional e sua aplicação em segurança imunológica. Disponível em:http://www.las.ic.unicamp.br/paulo/teses/20030226-MSc-Marcelo.Abdalla.dos.Reis-Forense.computacional.e.sua.aplicacao.em.seguranca.imunologica.pdf. Acessado

Reis, M., A. & Geus, P., L. (2002) *Analise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas.*Disponível em:http://www.las.ic.unicamp.br/paulo/papers/2002-Pericia-marcelo.reisforense.tecnicas.procedimentos.pdf#search=%222002-Pericia-marcelo.reis forense.tecnicas.procedimentos%22. Acessado em: 04/09/2010.

Sêmola, M.(2007). *COLUNISTAS*: Firewall. Disponível em:http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2007-06-28.7113160856/. Acessado em: 11/08/2010.

Vargas, R., G.(2006). Processos e padrões em perícia forense aplicada a informática. Disponível em: http://www.artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html. Acessado em:10/06/2010.

Outras Citações:

CONSTITUIÇÃO DE REPÚBLICA DE CABO VERDE, Julho, 2010.

Constituição da República de Cabo Verde (S/D). Disponivel em: http://www.presidenciarepublica.cv/conteudos/a_republica/constituicao_da_republica/. Acessado em: 15/09/2010.

Glosário

liveCD – é um CD que contém um sistema operativo (GNU/Linux, BSD ou outro) que não é necessário sua instalada no disco rígido do usuário uma vez que é executado directamente a partir do CD e da memória RAM.

Extensão .ibl – corresponde a Internet Binary Log (Log binário da Internet).

Snap-in – Consola de Gerenciamento Microsoft, também conhecido como MMC (Microsoft Management Console). É usado normalmente para acesso e configuração de alguns recursos de segurança do Windows.

ODBC – Open Database connectivity: é a abertura da conexão a base de dado.